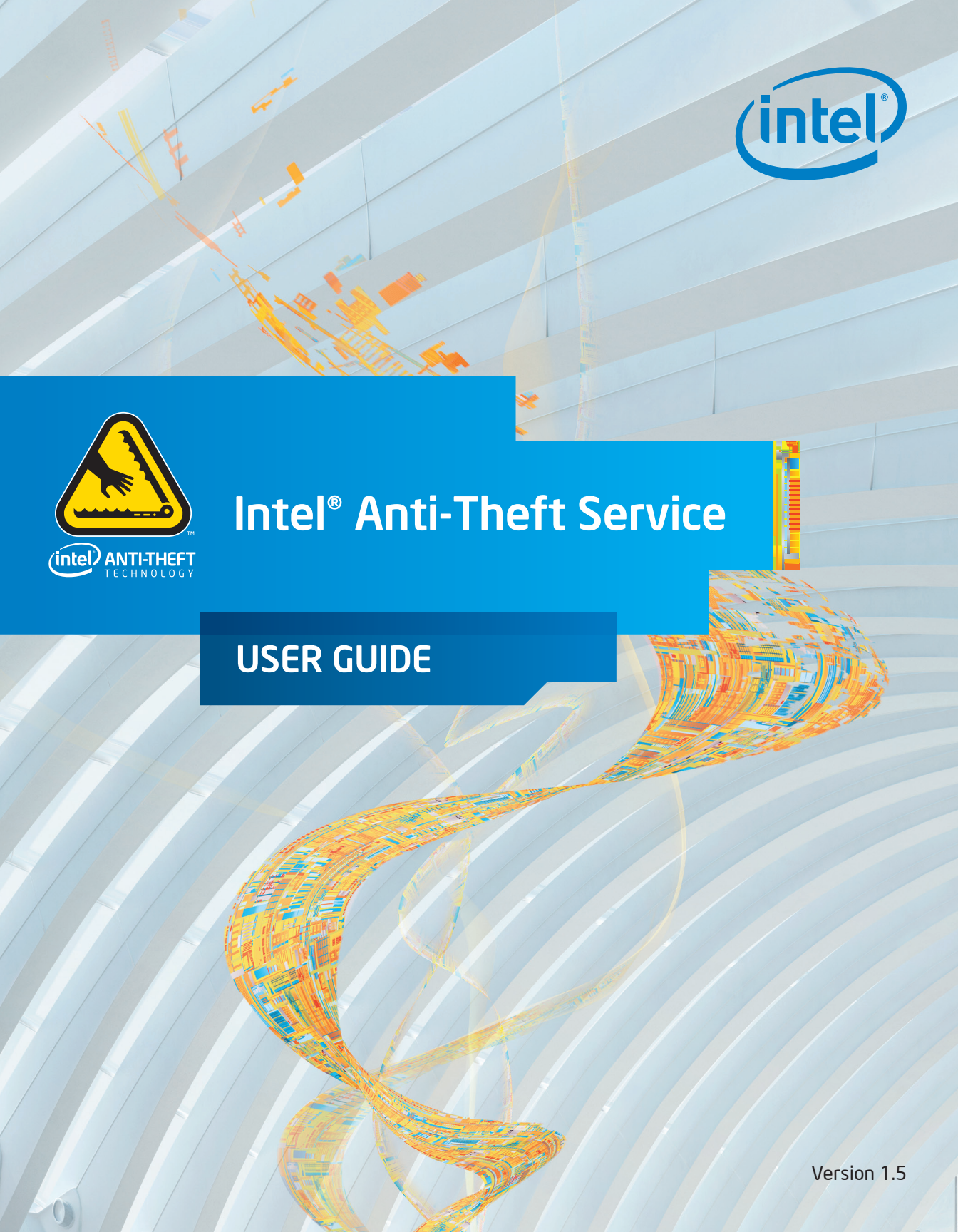


Intel® Anti-Theft Service

USER GUIDE

Version 1.5

Contents

CHAPTER 1:

Quickstart

If you understand the technology and you are comfortable with the features of this Service, follow this quickstart to set up and configure the Intel® Anti-Theft Service (referred to throughout as "the Service"). If you'd prefer more explanation with full details of the procedure, skip this section and go to the section "Introducing the Service."

Quickstart Requirements

To enable the Service, you need:

- A valid email address
- An Internet connection
- A laptop equipped with Intel® Anti-Theft Technology

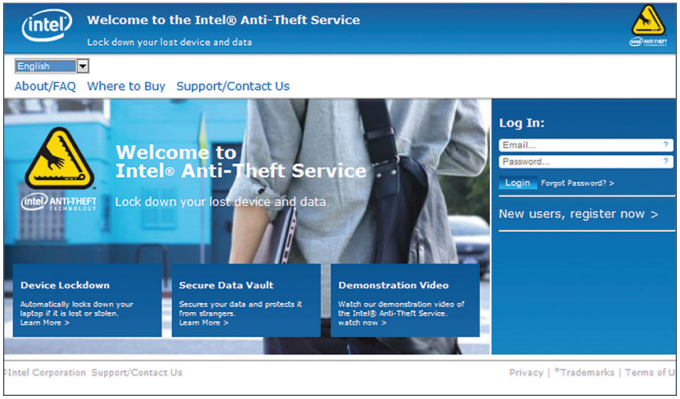
  Some of the capable models are listed here: ***ATservice.intel.com***

Quickstart Procedure

There are two basic steps to getting started:

1. Registering your laptop into the Service
2. Creating a Secure Data Vault container

NOTE: In certain locations, the Secure Data Vault feature is currently not available.



To register your laptop into the Service:

1. Go to **ATservice.intel.com**.
2. Click **New users, register now**.
3. Enter the information to set up your account.
4. Enter the six-digit code in the email that was sent by the Service.
5. Enter the information to configure your laptop.
6. Follow the instructions to complete the installation process.

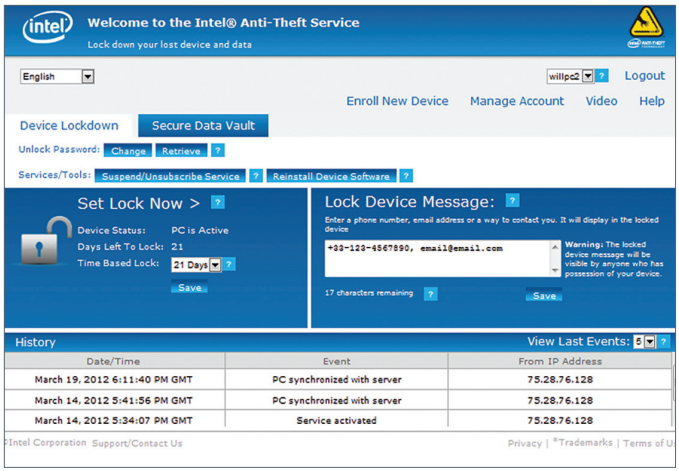
WARNING: Your laptop is not protected until you enroll it into the Service.

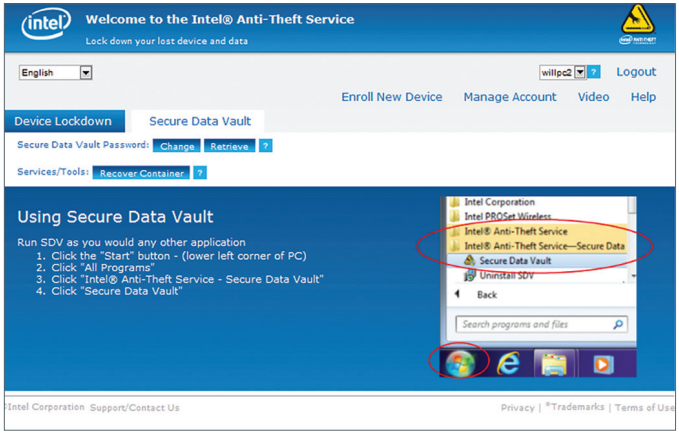
To create a Secure Data Vault container:

1. Click Windows **Start**.
2. Click **Secure Data Vault**.
3. Create a new Secure Data Vault password and container.
4. Move files into the container and the program will automatically encrypt the files.

To contact Intel Anti-Theft Service for additional questions:

Visit ATservice.intel.com. Click **Contact Us**.





CHAPTER 2:

Introducing the Service

Congratulations

Your selection of the Intel® Anti-Theft Service is a positive step toward guarding against theft and ensuring your personal privacy. This user guide explains how to take advantage of the built-in hardware features, software options, and service benefits.

Service Features

The Service lets you:

- **Lock down** your laptop if it is lost or stolen so that no one can use it
- **Create an encrypted folder (known as Secure Data Vault)** on your laptop where private files can be stored

NOTE: In certain locations, the Secure Data Vault feature is currently not available.

These features can't be used until you've registered your laptop, so be sure to complete the registration process promptly.

NOTE: Encryption converts data into a code to prevent unauthorized access.

More About the Built-in Protection

Your laptop includes built-in hardware components, designed by Intel, that work with software and the Service to provide multiple levels of protection. Intel® Anti-Theft Technology, available in all Ultrabook™ devices and on select laptops featuring the 2nd generation Intel® Core™ processor family, strengthens security by performing operations in protected areas in the laptop's hardware. Hardware-enabled protection enhances protection.

If your laptop is lost or stolen, it can be automatically disabled and only you can turn it back on.

It's like having a full-time security guard inside your laptop. When suspicious activities are detected, the technology automatically locks down your laptop.

If your laptop is lost or stolen, it can be automatically disabled and only you can turn it back on.

Laptop lockdown can occur in two ways:

1. **Your laptop is lost or stolen, and you notify the Service.** Your laptop will lock down the next time it synchronizes with the Service—no matter where it is. Your laptop automatically synchronizes with the Service whenever your laptop connects to the Internet.
2. **You don't connect your laptop to the Internet for a specified number of days** (as set in the Service options). For example, if your laptop is lost and the timer expires after several days without server synchronization across the Internet, the laptop goes into lockdown mode.

NOTE: We recommend that you complete the registration process as soon as possible so that the powerful anti-theft capabilities in your new laptop will be activated and ready for use.

You'll enjoy a greater degree of security and freedom with these strong laptop protection features in place, and you'll reduce the risk of identity theft or having private information revealed.

Secure Data Vault

Secure Data Vault is technology that creates a protected region on the hard disk drive of your laptop where you can securely store sensitive information. This region is identified by its own assigned drive letter on your system, and it can be accessed only by supplying the password that you create. All data contained in Secure Data Vault is encrypted, so it cannot be read by anyone other than you.

This feature automatically installs during the initial setup of the Service.

Setting up Intel® Anti-Theft Service for Your Laptop

You can control how the Service features work on your laptop by setting certain options. Spend some time becoming familiar with these options by reading the descriptions in this guide. This will help you understand how to configure the Service to your personal preferences.

CHAPTER 3:

Registering the Laptop into the Service

To register into the Intel® Anti-Theft Service, you need:

- An Internet connection and a valid email address
- A laptop that includes Intel® Anti-Theft Technology (when you enroll be sure to use the laptop that will be registered into the service, rather than any other laptop)

To begin the activation process:

1. Log in to **ATService.intel.com**.

The **Welcome** screen appears, described in the following section.

Step 1 – Setting up Your Account

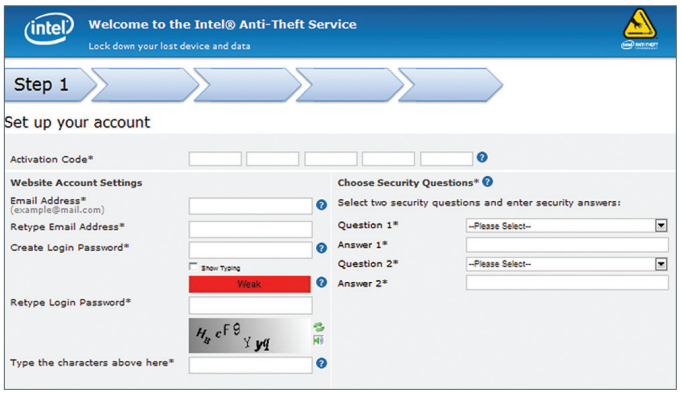
To register and enroll your laptop into the Service:

1. From the Welcome page, click **New users, register now**.

   The Account Set Up screen appears.

2. If you have an **Activation Code**, enter it exactly as it appears on the Activation Card inside the Intel® Anti-Theft Service Package.
3. Enter the **Email Address** you want to use for communications with the Service.
4. Create a **login password**. Use numbers and a mix of uppercase and lowercase letters—at least 8 characters in length—to make the password harder to break.

NOTE: The subscription activation site relies on Java*. Refer to the Appendix if you need details on how to set up Java for your laptop. This Appendix also provides information on browser compatibility and testing your laptop for service compatibility.



NOTE: The email address is used to complete the account setup.

5. Enter the characters shown in the graphics box near the bottom of the left column. This box helps confirm that a person, not a computer program, is creating the account.
6. Select two security questions to answer from the options at the top of the right column. Your answers are used to confirm your identity during subsequent visits to this site. Choose questions that you readily know the answers to (so that you can easily remember the answers).

NOTE: The visual indicator below the password box indicates the relative strength of the password that you're creating. A longer password using mnemonics rather than recognizable words is stronger.

7. Click the **I Agree to Terms and Conditions** link to read the legal details that apply to this account. If acceptable, select the check box to confirm your acceptance.
8. Click **Next** to complete setting up your account.

Step 2 – Verifying Your Email Address

The Service account server sends an email message to the email address you provided in order to validate the address.

> **NOTE:** If you stop the registration process after initially setting up your account, you can restart it by logging in with your email address and password.

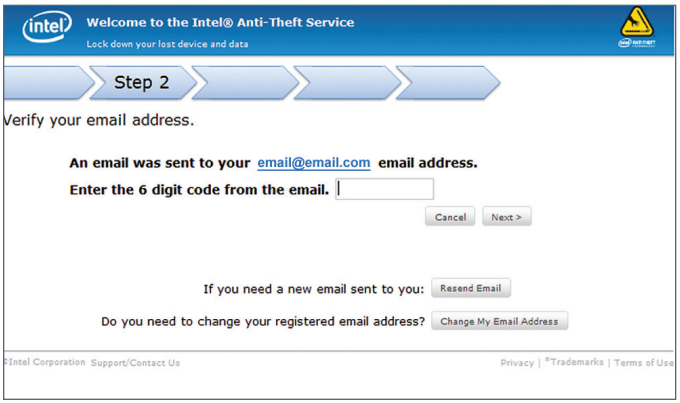
Open the email message sent to your registered email address. Enter the six-digit code from the email and click Next to verify your email address.

Step 3 – Configuring Your Laptop

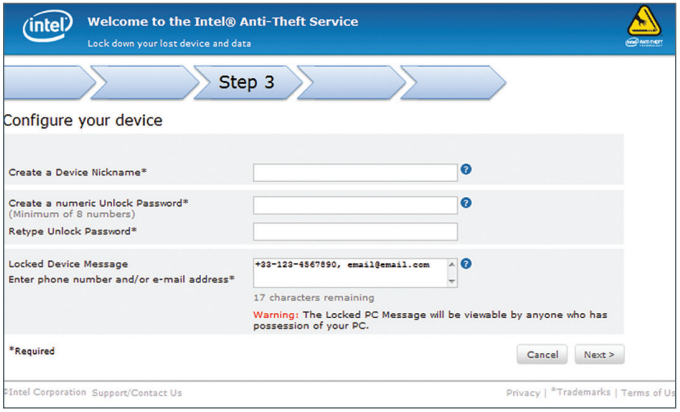
This step configures your laptop for the lockdown function.

> **NOTE:** You can change your email address by clicking **Change my Email Address**.

1. Select a nickname for the laptop that will make it easy to identify (for example, "Joe's computer" or "Dad's computer").
2. Create an Unlock Password of at least eight numbers. This will be the password used to reactivate your laptop following a lockdown event (for example, if the laptop is lost and then returned to you).



3. Enter a phone number or email address or both. The maximum message length is 50 characters, and only ASCII characters (i.e., 0 to 9, a to z, A to Z) are allowed. *Any information that you enter here will be visible to someone who has stolen your laptop.*
4. Click **Next** to apply the settings on this page to your laptop's lockdown function.



Step 4 – Downloading and Installing the Laptop-based Software

1. To start the download process, click **Next**.
2. A pop-up box shows the target folder for the installation in the **Select Destination Folder** dialog. You can select a different folder using the change button. Click **Next** when you have decided on the folder.
3. When the Service has finished the installation, it displays a summary screen that lists important information that applies to your account. We recommend that you print this screen and keep it in a safe location. It includes password details, the original Activation Code (if applicable), your unlock password, and other details that are essential for using the features of the Service.

Registering Multiple Laptops

You may register up to 10 different laptops on your account as long as you have an activation code for each laptop and the laptop is enabled to support Intel Anti-Theft Technology.

To register a new laptop:

1. Log in to the service with the laptop that will be registered into the service.
2. Click **Enroll New Device**.
3. Configure the new laptop.
4. Download and install the software onto the new laptop.

CHAPTER 4:

Using the Service

Whether you have one laptop or several enrolled in the Service, it is always easy to log on, check the current status of your enrolled laptops, make changes to passwords, view recent activities, and change the settings that apply to lockdown.

Locking Your Laptop

On a regular basis, when you turn on a laptop that is enrolled in the subscription service, that laptop automatically communicates or synchronizes with the Service server while it is connected to the Internet. This connection confirms that all is well and that no lockdown requests have been received (by phone or Web). If the lock or theft protection mode for the laptop is activated, one cannot go farther than the initial screen where the Unlock Password is required. (See Chapter 6, **Recovering your Laptop**.)

Requesting Lock Laptop Mode

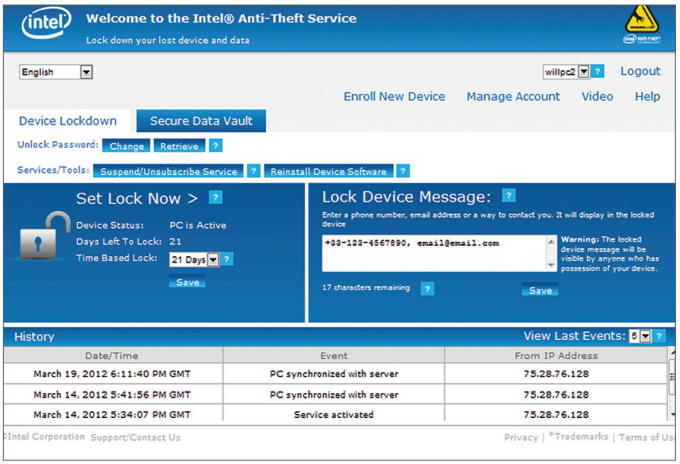
1. Login to your account and select the desired laptop from the drop-down menu.
2. Click **Set Lock Now**.

   The **Lock Laptop** dialog box appears.
3. Click the red **Lock PC** button.

   The lock request will be delivered to your laptop the next time it synchronizes with the server.

If you want to lock immediately (so you can see how the laptop behaves and view the lock screen), a pop-up box appears to show how to lock the laptop immediately.

After your laptop has shut down, see chapter 6, **Recovering your Laptop** to unlock your laptop.



TIP: To strengthen the security protection, configure your laptop so that the WLAN connection can be completed before Microsoft Windows* starts. This allows the contact with the Service server to be made (and any recent changes to the settings to be implemented).

Triggering the Lock/Theft Protection Mode

Locking Your Laptop Automatically

The laptop goes into a lockdown state if there has been no communication to the Service server within a number of days (as specified by the Timer Based Lock setting). You can set the number of days allowed before this action takes place by going to the Settings page.

For example, if your laptop is lost during travel on an airline and is sent to lost and found, after the set number of days passes without a network connection, it will lock down. If you set the lockdown value at 4 days, if the laptop is powered up on day 5, it will be in lockdown mode.

Updating the Timer Based Lock Setting

1. Login to your account and select the desired laptop from the drop-down menu.
2. Change the Timer Based Lock setting. You can also disable it.
3. Click **Save** to update the Timer Based Lock. The updated Timer Based Lock setting will be delivered to the laptop the next time it synchronizes with the server.

If you would like the settings to take effect immediately, a pop-up box appears to show how to synchronize the laptop immediately.

WARNING: Disabling Timer Based Lock will reduce your protection. This action enables an unauthorized person to remove Intel Anti-Theft Service software from your device, thus preventing you from locking it down in the event of a theft.

Setting the Lock Device Message

When the laptop is locked down, the screen shows the Lock Device Message.

1. Login to your account and select the desired laptop from the drop-down menu.
2. Change the Lock Device Message in the box provided.
3. Click **Save** to update the Lock Device Message. The updated message will be delivered to the laptop the next time it synchronizes with the server.

NOTE: You can also lock down your laptop by phone. Refer to the section "Getting Phone-based Support" for details.

If you would like the message to be updated immediately, a pop-up box appears to show how to synchronize the laptop immediately.

Checking Status through the Notification Area Icon

When the laptop-based software for the Service has been installed on your laptop, an icon appears in the Windows notification area (at the far right of the taskbar). This icon changes to reflect current status and to provide security- related notifications. The table on the following page describes the range of notifications and the icons in use.

Icon	Icon state	Notification	Action
	**Red**	Indicates that less than 24 hours remain before server contact is needed.	Log on to the Internet within the 24-hour window to avoid having the system lock.
	Pop-up balloon	Appears once each hour, counting down the time before the laptop automatically locks up. When less than 45 minutes remain, the balloon pops up every 15 minutes.	Log on to the Internet within the time specified to avoid having the system lock.
	**Gray**	Indicates the Service is currently suspended.	No action needed.
	Missing icon	If no icon is visible in the system tray, the laptop has been unsubscribed from the Service.	Re-enroll if service is needed.
	**Default icon**	Indicates the Service is enabled and monitoring conditions.	No action needed.

NOTE: The notification area icon may not be visible. Press the UP ARROW key to view the visible icons.

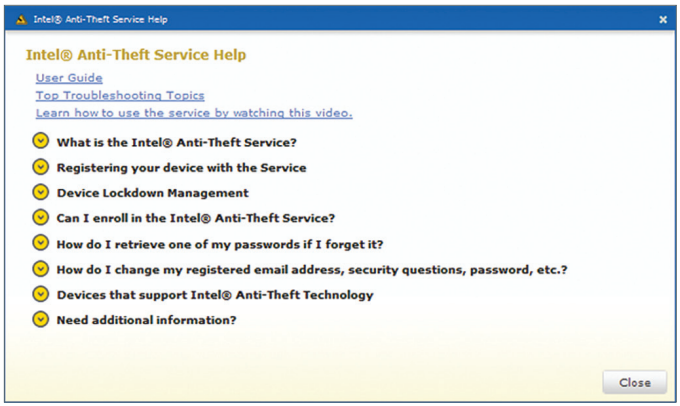
Right-Clicking the Notification Area Icon

If you right-click the notification area icon for the client application, you can access a menu that controls these options:

- **Open Secure Data Vault** (if closed) or **Close Secure Data Vault** (if open). Provides access to password-protected encrypted containers that you have created with the Secure Data Vault feature.
- **Synchronize Settings with Server.** Forces synchronization with the Service server to check status and update settings.
- **Software Update Settings.** Lets you select the manner in which updates are handled. Options include **Install Updates Automatically**, **Notify Me When an Update is Available**, and **Don't Automatically Check for Updates**. The command **Check Now** when selected immediately performs the check for updates.
- **Show EULA.** Displays the End User License Agreement.
- **Server Synchronization Status.** Indicates the current details related to the server synchronization operations.
- **About.** Provides information about the Service client application.
- **Exit.** The Service client application exits and the icon disappears from the tray. The client and system tray icon are again available the next time the laptop boots.

Using the Help Menu

You can obtain help when logged in to the Service by clicking the **Help** button near the top of the main screen. The Help window that appears offers answers to common questions and provides concise procedures for tasks such as creating a user account and enrolling a new laptop.



Viewing Tooltips

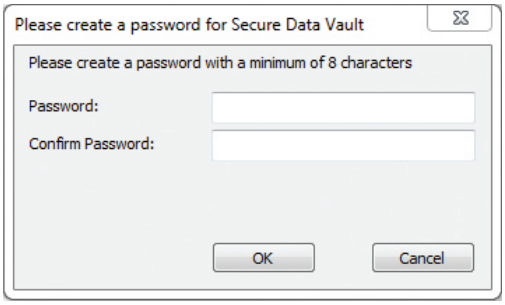
Many of the options displayed in the Service screens use tooltips to provide a quick description of a field or featue. To view tooltips, let the cursor hover over an item for two or three seconds and, if a tip is available, a pop-up description will appear.

CHAPTER 5:

Using Secure Data Vault

With Secure Data Vault, you can create a protected area on your hard disk that is password-protected and encrypted. Secure Data Vault offers additional protection for any private or sensitive information stored on your laptop.

NOTE: In certain locations, the Secure Data Vault feature is currently not available.



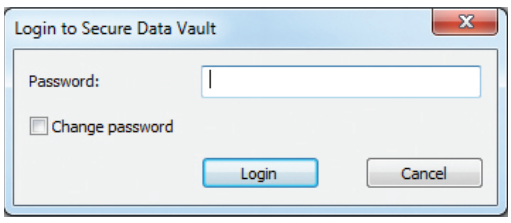
To use Secure Data Vault, you create an encrypted container, which appears as a drive on your laptop mapped to a letter that you assign to it (for example, drive E). When you start Secure Data Vault for the first time, you will need to create a password and the encrypted data can be accessed only if the password is supplied.

Opening Secure Data Vault

When Secure Data Vault is open, you can create containers and copy files into them. When the vault is closed, the files are encrypted and cannot be viewed unless the correct password is provided.

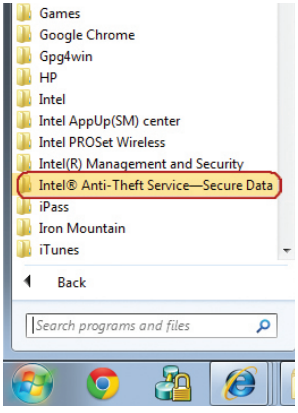
To open Secure Data Vault:

1. Locate the application for Secure Data Vault on your **Start** menu and click its icon. If you have not already created a password to access Secure Data Vault, the program will ask you to create one at this time.
2. Enter the password you want to use and confirm this entry in the next field. Click **OK** to continue.



NOTE: We strongly recommend that you regularly back up the files in your Secure Data Vault using your favorite backup utility. You can also back up the entire encrypted container, but the container is typically large and could require a significant amount of time and space for the back-up process. Information in this backup will have the same encryption and password protection as the encrypted container that you created on your hard disk. If your laptop is stolen or lost, you can recover the information from the backup using the data recovery tool.

3. In the **Login to Secure Data Vault** dialog box, type the password, and then click **Login**.
4. In the window that appears, select the name of the container that you want to open.
5. Click the **Open** icon to make the container, associated with the drive letter you assigned, available for use. If you haven't yet created any containers, the next section explains how to do so.



Creating an Encrypted Container

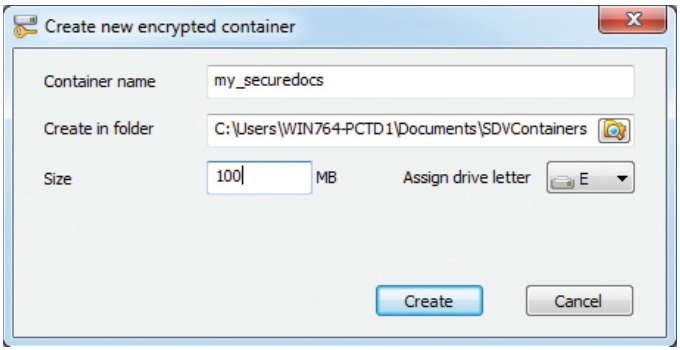
You can create as many containers as you want within Secure Data Vault.

To create a new encrypted container:

1. Select the application for Secure Data Vault from the **Start** menu on your laptop.
2. From the main window, select **New**.

   The **Create New Encrypted Container** dialog box appears.
3. Create a name for the new container and designate a folder in which to store it. By default, the encrypted container is stored in your **My Documents** folder on drive C. Use the Browse button to select a different folder anywhere on your system.
4. Specify a size for the container in the **Size entry** field. Make sure that you leave adequate space on your disk drive for other applications and normal operations.

NOTE: If you choose to back up the entire container, the size of the container will determine the time and space that the backup will take. To expedite backup time and to save space, you can back up your files instead of the entire container. A large container typically requires a significant amount of time and space to backup.



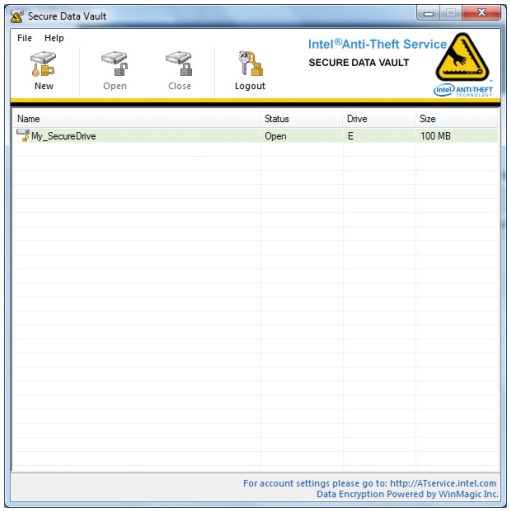
1. In the **Assign drive** letter field, specify the letter drive you want to use.
2. Click **Create** to name and create the encrypted container. The drive that you assigned to the container and the status will be shown in the window for Secure Data Vault.

While the status of the container is Open, you can move files in and out of it as you would with any disk drive—using the Microsoft Windows* tools that are most convenient. Files are encrypted from the time they are moved into the vault.

1. Click the **Close** icon to return the vault to password protection.
2. Click the **Logout** icon to close the application.

Logout button closes all containers and then logout from SDV. This can be useful if you have several containers opened.

NOTE: You can include the path for each Secure Data Vault encrypted container in your regular backup operations, but the entire container will be backed up. This should be the path where Secure Data Vault was originally created (for example: C:\User\Administrator\Documents\SDVContainers). The data contained in the backup will also be encrypted, and it can be recovered using the recovery procedure described in the following section.



Closing Secure Data Vault

To close Secure Data Vault:

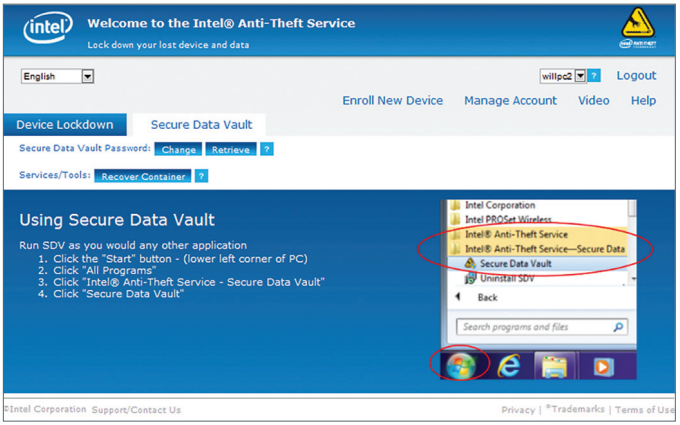
1. Once you're done using Secure Data Vault and you've finished copying files in or out of containers, select any open containers that you'd like to close from the displayed list.
2. Click the **Close** icon to close and lock the selected container.
3. Click the **Logout** icon to exit from the application for Secure Data Vault.

Recovering Secure Data Vault Information

If your laptop is lost, stolen, or suffers a hard disk drive failure, you can recover the data stored in your Secure Data Vault if you have a backup file available.

To restore Secure Data Vault on a replacement laptop:

1. On your replacement laptop, restore the data backup of the Secure Data Vault encrypted container to the **My Documents** folder.
2. Log in to the Service, select the desired laptop from the drop-down menu, and then click the **Secure Data Vault** tab.
3. Click the **Recover Container** button to download the data recovery tool for Secure Data Vault.



4. When the download is complete, double-click the tool to open it. If you've restored the container files to **My Documents**, the recovery program will automatically recognize and register them.
5. Open any of the displayed containers and copy the recovered content to any appropriate location on your hard drive or other media.

If your replacement laptop includes Intel® Anti-Theft Technology capabilities and you have service time remaining, you can optionally enroll the laptop in the Service at this time.

To restore Secure Data Vault on your laptop following hard disk replacement:

1. Complete the installation of the new hard disk drive or operating system upgrade.
2. Restore the data backup of an encrypted container made by Secure Data Vault to the **My Documents** folder on your laptop.
3. Log in to the Service, select the desired laptop from the drop-down menu, and click **Recover Container** to download and install the container.

4. When the software has been installed, open the Secure Data Vault application. Your encrypted container files that have been copied to the **My Documents** folder are visible and ready to access.

If your laptop has been repaired, had changes to its motherboard, or had the BIOS re-flashed (causing the laptop to become un-enrolled), the system may be returned in a suspended state. When you resume the Service, we recommend that you change your password.

To restore Secure Data Vault on your laptop after a repair:

1. Restore the data backup of the container made by Secure Data Vault to the **My Documents** folder on your laptop.
2. Log in to the Service, and then select the **Secure Data Vault** tab for the selected laptop.
3. Click **Recover Container** to download the data recovery tool for Secure Data Vault.
4. When the download is complete, double-click the tool to open it. If you've restored the container files to the **My Documents** folder, the recovery program will automatically recognize and register them.
5. Open any of the displayed containers and copy the recovered content to any appropriate location on your hard drive or other media.

NOTE: The Export/Import functionality can also be used for recovery purposes, to backup and restore a particular container. This is a simpler backup/recovery procedure.

Secure Data Vault

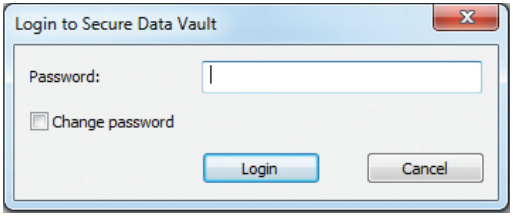
If you lose or forget the password to Secure Data Vault, you can retrieve it as long as your Service subscription is active.

To retrieve the password for Secure Data Vault:

1. Log in to the Service and then click the **Secure Data Vault** tab for the selected laptop (on which Secure Data Vault is stored).
2. Click **Retrieve Password**. A message containing a link is sent to your current email address.
3. Open the email message, and then click the link provided.
4. Answer the security questions on the screen that appears. The program then lets you view the current password.

NOTE: If your subscription is not active, your Secure Data Vault is in read-only mode and you cannot recover your password. For more details, refer to Chapter 7: **Suspending or Cancelling Service**.

NOTE: You can change the password for Secure Data Vault by selecting the Change Password check box at the time you log in to Secure Data Vault. The program will provide a second field to confirm the newly entered password. The next time the client application synchronizes with the Service, this new password will be stored on the server. You can then retrieve it whenever necessary using the preceding procedure.



CHAPTER 6:

Recovering Your Laptop

If your laptop is lost or stolen, it can be locked in one of three ways:

- By logging into the Service and using the **Set Lock Now** laptop command
- By the laptop failing to connect with the Service for the set number of days in the Timer Based Lock
- By issuing a Lock laptop command by phone using Customer Support

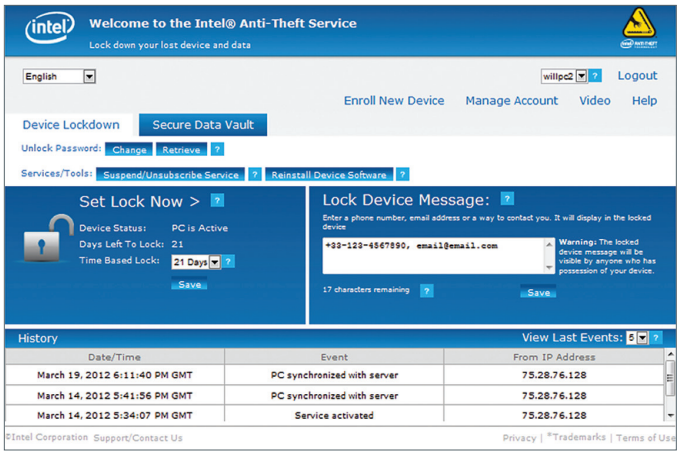
Unlocking from the Web

If your locked laptop is recovered, you can return it to normal operation by first setting the laptop to unlock on the Web and then entering the Unlock Password on the locked laptop.

To unlock the laptop on the Web:

1. Log in to the Service with another laptop, and then click the name of the selected laptop. The values that apply to that laptop are shown in the user interface.
2. Click the **Set Unlock Now** button.
3. Click **Unlock PC** to set the laptop to unlock.

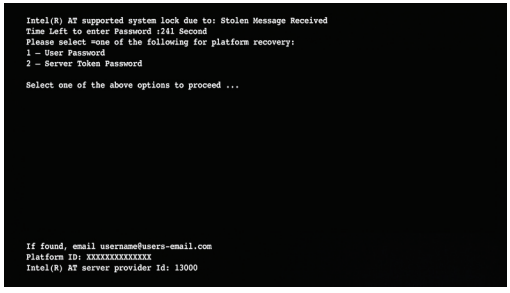
The next time the specified laptop communicates with the Service, it will be unlocked for your use. The laptop will communicate when it powers up or on regular intervals.



Entering the Unlock Password

To enter the Unlock Password:

1. Turn on your laptop. If the laptop has been locked, a screen will appear from the BIOS that requests the recovery passphrase, such as the one shown below:
2. Type: 1 (to use a passphrase).
3. Enter the passphrase (your Unlock Password). If the password is correct, the laptop completes the startup process.



Retrieving the Unlock Password

If you forget the Unlock Password, you can retrieve it from the Service.

To retrieve the Unlock Password for an enrolled laptop:

1. Log in to the Service, and then click the name of the selected laptop.
2. Click **Retrieve Password**. A message with a link is sent to your registered email address.
3. Click the link and then answer the security questions. The Service displays your Unlock Password.
4. Click OK to return to the previous screen.

Recovering the Service

In certain situations, your subscription to the Service may be current, but you may not be able to access it because of disk-drive corruption, a hard disk change, or other system changes. To continue using the Service, you will need to log in and reinstall the necessary software.

To recover the Service:

1. Log in to the Service, and then click the name of the selected laptop.
2. Click **Reinstall Device Software**

CHAPTER 7:

Suspending or Cancelling Service

Depending on circumstances, you may want to temporarily suspend the Service. For example, if you take your laptop in for service, you don't want it to lock while being repaired. In such cases, you can use the Suspend feature to temporarily discontinue service and then use Resume when you return to re-activate the anti-theft coverage.

Suspending Service

To suspend service:

1. Log in to the Service, and then click the name of the laptop that you want to suspend.
2. Click the **Suspend** tab.
3. Click the Suspend button in the pop-up box to verify.

   The Service suspension takes place the next time the laptop synchronizes with the Service.

If you want the Service to be suspended immediately, a pop-up box appears to show how to synchronize the laptop.

To operate from Suspend Mode:

1. Starting from Shutdown or Hibernate mode, the laptop will show the following:
2. Type **n**, and then press **Enter**.

   The laptop will resume normal operation.

To resume service:

1. Log in to the Service, and then click the name of the laptop for which you want service resumed.
2. Click the **Suspend** button.
3. Click the **Resume** button in the pop-up box.

The Service is resumed and the timers for the automatic lockdown settings that you have specified begin counting once more after the laptop has synchronized with the Service.

If you want the Service to be resumed immediately, a pop-up box appears to show how to synchronize the laptop.

NOTE: While suspended, your laptop does not respond to automatic lockdowns or lock requests. As an alternative to suspending services, you can disable the Timer Based Lock.

Unsubscribing

You can cancel your subscription at any time. Unsubscribing turns off the theft protection features for your laptop.

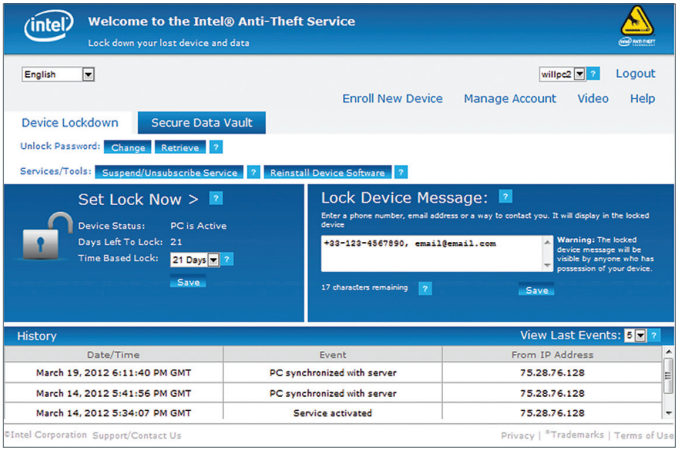
To unsubscribe from the Service:

1. Log in to the Service, and then click the name of the selected laptop.
2. Click the **Suspend/Unsubscribe** button.

The following dialog box appears.

3. To cancel the subscription service, click **Unsubscribe/Uninstall** and then answer the security questions that appear.
4. Confirm this change in the dialog box that appears.

If you have an Activation Code, you can re-activate the Service subscription by supplying the original Activation Code within the time limit of your original subscription period. Otherwise, if you have a trial service or no activation code, you may not re-activate the Service.



If you want the Service to be unsubscribed immediately, a pop-up box appears to show how to synchronize the laptop.

If you unsubscribe, files that you have stored in Secure Data Vault will still be protected, but without hardware security. **We recommend that you move your secure data out of Secure Data Vault to another location before you unsubscribe.**

CHAPTER 8:

Contacting Customer Support

Support Options

If you need answers to questions not covered in this user guide, or you would like to configure your laptop (such as locking your laptop) with the help of an agent, visit the ATservice.intel.com site and click **Support/Contact Us**. With the options provided you can:

1. Email questions about the Service or provide feedback
2. Chat with a live agent (during certain hours)
3. Call Customer Support. Individual phone numbers for each country or region are listed on the site, ATservice.intel.com.

To talk to a service representative:

1. Call the phone number for your country or region. A full list of current numbers appears on the ATservice.intel.com site. Click **Support/ Contact Us** to find the appropriate number.
2. Explain the nature of your request to the service representative.

NOTE: If you receive support from the retailer from whom you purchased the laptop, that retailer will have its own privacy guidelines

CHAPTER 9:

FAQ

What is Intel® Anti-Theft Service?

The Service helps consumers protect their laptop and data from theft. This Service uses Intel® Anti-Theft Technology (Intel® AT) as a foundation and provides added security built into the chipset. Additionally, this service lets you use an optional feature called Secure Data Vault on your laptop where private files can be encrypted and stored.

NOTE: In certain locations, the Secure Data Vault feature is currently not available.

What is Intel Anti-Theft Technology?

Intel AT locks down your laptop if it's lost or stolen and helps secure sensitive information stored on the laptop's hard drive.

Intel AT has these benefits:

- **Built-in protection for added peace of mind:** This technology is built into Intel's chips so reformatting or replacing the hard drive will not defeat the lock.
- **Easy to disable the laptop locally or remotely when lost**: Lock down your laptop if it is lost or stolen. A locked laptop cannot be used by a thief, but can be easily unlocked by its owner.
- **Laptop theft deterrence:** The Intel AT sticker warns thieves that the laptop has added protection. This can help in deterring theft.

How is privacy protected for the enrollment and account information?

All user information is stored in encrypted form on the Service server.

NOTE: If you have multiple laptops, you must first select the correct laptop to continue. Several other functions are available by phone, including Lock, laptop Status, Retrieve Login Password, and Talk to Agent. Follow the voice prompts to access the services that you need.

Does the Service include recovery of a lost or stolen laptop?

The Service does not provide recovery of lost or stolen laptops. Guaranteed laptop recovery is not feasible, so the Service focuses on deterring theft and then disabling stolen laptops and protecting their data. Your customized lock message may make it possible for someone to return your laptop.

Account Settings

Why do I have to create an account and enroll my laptop?

You must create an account to use the Service to control security, validate your identity, and assist in performing lock and unlock procedures. The activation code is used to create an account.

Who can see my account information?

Only the valid account holder and customer support representatives for the Service can view account information. Users must log in to the Service Web site to view information about any laptops that have been enrolled in the Service. Additional information about the current account settings appears in the Account Settings window on the Web site, which can be accessed by answering the authentication questions (based on the information supplied initially by the user).

How is my account information used?

Account information—such as your email address—is used by the Service to notify you of relevant information about your enrolled laptop.

How is my email address used?

Your email address is the basic means for communication with the Service. Messages are generated to the address you provide to confirm and validate certain operations, such as resetting your account password, retrieving a password, providing warnings about missed synchronizations with the server, issuing service expiration notices, and so on.

How can I change my email address?

To change your email address, log in to the Service, select Manage Account, and answer the authentication questions to gain access. You can change your email address on the screen that appears.

What is the Login Password?

The Login Password controls access to your Service account. You must supply this password each time you visit the Web site.

How do I change my Login Password?

To change your login password, log in to the Service, select Manage Account, and answer the authentication questions to gain access. You can make the changes in the window that appears. You can also reset the password using the Forgot Password option on the home page of the Web site. The Service sends a message to your registered email address. When you receive the message, follow the link contained in it to complete the password reset process. You will need to answer authentication questions to confirm the reset.

How are my Login Password and Unlock Password different?

The Login Password gives you access to log in to the Service. The Unlock Password is used only in situations where your laptop is locked down and you want to unlock it (for example, if the Timer Based Lock is triggered after the set number of days, which locks down the laptop). An additional password that applies to Secure Data Vault is also kept available for retrieval on the site.

How do I choose a strong Login Password?

A strong login password consists of:

- At least 8 characters
- One or more numerals
- An uppercase and lowercase character
- A special character
- The password does not start with a question mark (?) or exclamation mark (!), or 3 repeating characters at the beginning

When you first create your Login Password, a graphic gauge below the password entry box dynamically shows the strength of the password as you add characters.

What are Authentication Questions?

Authentication questions are combinations of questions and answers that you define as a user when you register. They provide extra security whenever you are accessing or changing sensitive information within your account. **We recommend that you memorize the answers to the questions and keep them secret to maintain the security of your account.**

I already have an account. Can I add a new laptop to it?

Any current subscriber with a valid account can add up to 10 laptops as long as an activation code is available for each enrolled laptop. To add a laptop to your account, log in to your account, and use the Enroll laptop button on the Service home page.

Theft Policy Settings

What does the term Timer Based Lock mean?

Each day that a laptop does not communicate with the Service server counts as one day toward automatic lockdown, based on the Timer Based Lock value that has been set. For example, if the timer value is set to 10 days and your laptop doesn't communicate with the server on the Internet for 6 days, the notification area icon will notify you that 4 days until automatic lock remain. You can use your Unlock Password if your laptop is locked down inadvertently.

What does Locked Laptop Message mean?

If the laptop has been locked down and someone tries to start it, the BIOS displays the Locked Laptop Message that you specified when enrolling your laptop.

What is Unlock Password?

Use the Unlock Password to gain access to a laptop that has been locked down. This password is set during the laptop enrollment process.

How do I change my Unlock Password?

To change the Unlock Password, log in to the Service, and then click the Change button to enter a new password.

I forgot my Unlock Password. How can I retrieve it?

To retrieve your Unlock Password, log in to the Service, and then click the Retrieve Password button to enter a new password. The Service generates an email message containing a link. Click the link to complete the process, which includes answering authentication questions to validate your identity. The Unlock Password is displayed for two minutes.

You can also recover your Unlock Password by contacting the Interactive Voice Response support line.

Secure Data Vault

What is Secure Data Vault?

Secure Data Vault is a data protection service that lets you create an encrypted container on your laptop's hard drive where sensitive files can be protected and stored.

NOTE: In certain locations, the Secure Data Vault feature is currently not available.

Does Secure Data Vault protect all the data on my laptop?

No. Secure Data Vault protects only the files that are copied to it.

How does it prevent others from seeing my data?

The encrypted data stored in Secure Data Vault can be accessed and decrypted only by supplying a password. Only an authenticated user can access the files stored in the vault.

What kind of files or data should I store here?

Secure Data Vault can be used to store any kind of files or documents that you want to protect from unauthorized viewing. This might include bank or credit card information, passwords for other accounts, personal information that might be used for identity theft, or anything you want to encrypt.

Unlock Password

How do I lock a lost or stolen laptop?

To lock a lost or stolen laptop, log in to the Service, select the name of the laptop that you want to lock and click the Set Lock Now button for the enrolled laptop. Then, click the Lock button. Following the next synchronization with the server (if someone tries to start up the laptop), the laptop will be locked by the Service. You can also call customer support to lock a laptop.

How do I unlock a laptop?

Then log in to the Service from a different device, select the name of the laptop that you want to unlock, click the Set Unlock Now button for the enrolled laptop, and click the Unlock button. Turn on the laptop and enter the Unlock Password on the BIOS screen that appears. Following the next synchronization with the server, the laptop will be unlocked by the Service.

How do I suspend or resume the Service?

To suspend service, log in to the Service, and then select the name of the laptop that you want to suspend. Click the Suspend/Unsubscribe button and then click the Suspend button again to verify. While suspended, your laptop does not respond to automatic lockdowns or lock requests. Note that you will need to answer the security questions to suspend service.

To resume service, log in to the Service, and then select the name of the laptop for which you want to resume service. Click the Suspend button, and then click the Resume button.

How do I view the history for an enrolled laptop?

To view the Service history for a laptop, log in to the Service, select an enrolled laptop, and the last five events related to this laptop will be displayed. To see more events, select the number of events in the drop-down menu.

How do I unsubscribe a laptop from the Service?

Log in to the Service, and then click the name of the selected laptop. Click the Suspend/ Unsubscribe button. Click the Unsubscribe/ Uninstall

button in the dialog box that appears. The next time the server synchronizes with the laptop, the laptop subscription will be terminated. Note that you will need to answer the security questions to unsubscribe from the Service.

APPENDIX

Installing Java* Runtime Environment v6

The Service requires that Java* Run Time Environment (JRE) version 6 be installed for Web pages to be viewed properly. If JRE v6 is not installed you may see a blank screen when trying to access a page or the following dialog box may appear in your browser window.

In most cases, Java will already be installed and enabled for your browser, but if you receive a message that Java is needed to continue, complete the installation in the following manner.

To install JRE v6 in Internet Explorer*

1. 1Click the Windows **Start** button, and then click **Internet Explorer**. The browser window appears.
2. Access the Java.com Web site.
3. Click the **Free Java Download** button. The File Download – Security Warning appears.
4. Click **Run** to continue. The installer provides more details about the software.
5. Click **Run** to confirm. The **Welcome to Java** dialog box appears.
6. Click **Install** to proceed with the installation. A progress bar tracks the downloading and installation of the software.
7. After the installation has finished, restart the computer to enroll in Intel® Anti-Theft Service.

With Java installed, you should have full access to all pages on the Service site.

Checking Browser Compatibility

The Service works with the following browser:

- Microsoft Internet Explorer Version 8 and 9
- Chrome
- Firefox
- Safari

GLOSSARY

Account Password. When you first create your Service account, you assign a password to control access to it through the Service Web site. Protect this password carefully because it is the primary means of locking and unlocking your laptop and setting the options that apply to your account.

BIOS (Basic Input/Output System). A program stored within your laptop that controls startup operations and configures the laptop for use by the operating system. If your laptop is locked down by the Service, the complete startup operation can't proceed unless the Unlock laptop password is provided, preventing a thief from loading the operating system to access the files on your laptop.

Encryption. A process by which a code or cipher is used to conceal data for security purposes in a computer. The encrypted data becomes unreadable unless a key is supplied to access it (which can be tied to a password or other means of authenticating a user's identity).

Encrypted Container. A protected area on your hard disk drive that you create using Secure Data Vault. To your laptop, the area looks like a normal drive with a drive letter but the information within it is encrypted and protected by a password.

Intel® Anti-Theft Technology. Security features built into select 2nd generation Intel® Core™ processor family products that can protect sensitive data by blocking the boot process at startup.

Secure Data Vault. Technology that creates a protected area on a computer that can be used to store personal information in an encrypted format.

Secure Data Vault password. The password you create when you make a Secure Data Vault using the laptop-based software installed on your laptop. This password, which controls access to the encrypted data, is also stored on the server of the Service so that you can log in and access it, if needed.

Server Synchronization. A scheduled communication exchange between the laptop and the Service that compares settings, evaluates current conditions, and determines whether the laptop should be locked for security reasons.

Unlock Password. A password that you create through the Service that must be supplied to access a laptop that has been locked down for protection. This password should be carefully stored in a place where it can't be stolen and where it is available if the laptop is locked. If you lose it, your laptop may be unrecoverable.

No system can provide absolute security under all conditions. Intel® AT requires an enabled chipset, BIOS, firmware, software, and a subscription with a capable Service Provider such as Intel® Anti-Theft Service. Consult your system manufacturer for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft.

If your system is enrolled in the Intel® Anti-Theft Service (the "Service"), you must regularly connect your enrolled computer system to the Internet so that it can synchronize with the Service's system server. Lack of regular synchronization with the Service's system server can lead to your enrolled computer system being locked down which will require you to use your unlock password to unlock your computer system.

intel ANTI-THEFT TECHNOLOGY