



Windows Vista™

Windows Vista Beta 2 Trusted Platform Module Services Step-by-Step Guide

Microsoft Corporation

Published: December 2005

Abstract

Trusted Platform Module (TPM) Services is a new feature set in Microsoft® Windows Vista™ used to administer the TPM Security Hardware in your computer. TPM Services architecture provides the infrastructure for hardware-based security by providing access to and assuring application-level sharing of the TPM. This guide includes system requirements and step-by-step instructions on how to use TPM Services in a test lab environment.

Microsoft

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Vista, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

References to any third-party products or their hardware identifiers are for illustrative purposes only. These product is not endorsed by Microsoft Corporation.

All other trademarks are property of their respective owners.

Contents

Windows Vista Beta 2 Trusted Platform Module Services Step by Step Guide	5
What is Trusted Platform Module Services?	5
What is a Trusted Platform Module?	5
Who should use this guide?	6
In this guide	6
Requirements for TPM Services.....	6
Preparing the test lab for TPM Services	6
Key scenarios for TPM Services	7
Scenario 1: Initialize the TPM.....	7
Steps for initializing the TPM.....	7
Step 1: Turn on the TPM.....	8
Step 2: Set ownership of the TPM	9
Scenario 2 Turn off and clear TPM	10
Turn off the TPM	10
Clear the TPM.....	11
Scenario 3: Block and allow TPM commands	12
Logging bugs and feedback	13
Additional resources	13
Technology Adoption Program support.....	13

Windows Vista Beta 2 Trusted Platform Module Services Step by Step Guide

This Step-by-Step Guide provides the instructions necessary to use Trusted Platform Module (TPM) Services in a test lab environment.

What is Trusted Platform Module Services?

Trusted Platform Module (TPM) Services is a new feature set in Microsoft®Windows Vista™ used to administer the TPM Security Hardware in your computer. TPM Services architecture provides the infrastructure for hardware-based security by providing access to and assuring application-level sharing of the TPM.

What is a Trusted Platform Module?

A TPM is a microchip designed to provide basic security-related functions to the software utilizing it. The TPM is usually installed on the motherboard of a computer or laptop, and communicates with the rest of the system using a hardware bus.

Computers that incorporate a TPM have the ability to create cryptographic keys and encrypt them so that they can only be decrypted by the TPM. This process, often called "wrapping" or "binding" a key, helps protect the key from disclosure. On TPMs, the master "wrapping" key is called the Storage Root Key (SRK), and this key is stored within the TPM itself. This ensures that the private portion of the key is never exposed.

TPM-incorporated computers also have the ability to create a key that has not only been wrapped, but also tied to certain platform measurements such that the key can only be unwrapped when those platform measurements have the same values that they had when the key was created. This process is called "sealing" the key to the TPM. Decrypting it is called "unsealing." The TPM can also seal and unseal data that is generated outside of the TPM.

TPM-equipped computers are have increased resistance to attack in the same way that all hardware components are more resistant to attack than software. This is especially true in the realm of cryptographic key management. Private portions of key pairs are kept separated from the memory controlled by the operating system. Keys can be sealed to the TPM, so certain assurances about the state of a system (its trustworthiness) can be made before the keys are unsealed and released for use. Also, since the TPM uses its

own internal firmware and logical circuits for processing instructions, it does not rely upon the operating system and is not subject to external software vulnerabilities.

Who should use this guide?

This guide is intended for the following audiences:

- IT planners and analysts who are evaluating the product.
- Early adopters.
- Security architects who are responsible for implementing trustworthy computing.

In this guide

- [Requirements for TPM Services](#)
- [Key TPM Services scenarios](#)
- [Scenario 1: Initialize the TPM](#)
- [Scenario 2: Turn off and clear TPM](#)
- [Scenario 3: Block and allow TPM commands](#)
- [Logging bugs and feedback](#)
- [Additional Resources](#)

Requirements for TPM Services

We recommend that you first use the steps provided in this guide in a test lab environment. Step-by-Step guides are not necessarily meant to be used to deploy Microsoft® Windows Server™ Code Name "Longhorn" or Windows Vista features without accompanying documentation (as listed in the Additional Resources section) and should be used with discretion as a stand-alone document.

Preparing the test lab for TPM Services

The lab configuration needed for testing TPM Services is simply a client computer connected to an isolated network through a common hub or Layer 2 switch. The client must be running Windows Vista and be equipped with a compatible TPM (version 1.2) and Trusted Computing Group (TCG)–compliant BIOS. A portable USB memory drive is

also recommended. Private addresses should be used throughout the test lab configuration.

Key scenarios for TPM Services

This guide covers the following scenarios for TPM Services:

- [Scenario 1: Initialize the TPM](#)
- [Scenario 2: Turn off and clear the TPM](#)
- [Scenario 3: Block and allow TPM commands](#)

Note

The three scenarios included in this guide are intended to help administrators become familiar with the TPM Services feature set of Windows Vista. They include the basic information and procedures administrators need to start configuring and deploying TPM-equipped computers within their networks. Information and procedures for advanced or customized TPM Services configurations are not included in this guide.

Scenario 1: Initialize the TPM

This scenario details how to initialize the TPM on your computer. The initialization process involves turning on the TPM, and then setting ownership of the TPM. This scenario is written for local administrators responsible for setting up TPM-equipped computers.

Remote initialization of the TPM is supported in Windows Vista; however, a physical presence is required to turn on a computer's TPM. If a computer is shipped with the TPM turned on, no physical presence is required. Information about and procedures for remote initialization are not included in this guide. TPM Services exposes a management API that allows the procedures in this scenario to be performed through scripting. Information about scripting those tasks is also not included in this guide.

Steps for initializing the TPM

To initialize the TPM on your computer, complete the following steps:

- [Step 1: Turn on the TPM](#)
- [Step 2: Set ownership of the TPM](#)

Step 1: Turn on the TPM

The TPM must first be turned on before it can be used to help secure your computer. Step 1 covers the procedure for turning on a computer's TPM.

Computers manufactured to meet Windows Vista requirements include pre-boot BIOS functionality that makes it easy to turn on a computer's TPM through the TPM Initialization Wizard. Upon launching the TPM Initialization Wizard, you will be able to determine if the computer's TPM is turned on or off.

The following procedure steps you through the process of launching the TPM Initialization Wizard and turning on the TPM.

Note

To perform the following procedure, you must be logged into a TPM-equipped computer with local administrator credentials.

To launch the TPM Initialization Wizard and turn on the TPM

1. Click **Start**, click **Accessories**, and then click **Run**.
2. Type *tpm.msc* in the **Open** box, and then click **Enter**. The TPM Management Console is displayed.
3. Under **Actions**, click **Initialize TPM**. The TPM Initialization Wizard is launched.
 - If the TPM is turned off, the TPM Initialization Wizard will display the **Turn on the TPM Security Hardware** dialog box. This dialog box provides guidance for turning on the TPM.
 - If the TPM is already turned on, the TPM Initialization Wizard will display the **Create the TPM owner password** dialog box. See later in this guide.
 - If the TPM Initialization Wizard detects a BIOS that does not meet Windows Vista requirements, you will not be able to continue with the wizard, and you will be alerted to consult the computer manufacturer's documentation for instructions on turning on the TPM.
4. Click **Shutdown** (or **Restart**), and then follow the BIOS screen prompts.

Note BIOS screen prompts and controls will vary by computer manufacturer.
5. After restart, an acceptance prompt is displayed to ensure a present user, and not malicious software, is turning on the TPM.

Step 2: Set ownership of the TPM

The TPM must also be owned before it can be used to help secure your computer. By setting ownership of the TPM, you are assigning a password that helps ensure only the authorized TPM owner can access and manage the TPM. The TPM password is used to turn off the TPM if you no longer want to use it, or to clear the TPM if the computer is to be recycled. Use the following procedure to take ownership of the TPM.

The following procedure steps you through the process of setting ownership of the TPM using the TPM Initialization Wizard.

Note

To perform the following procedure, you must be logged into a TPM-equipped computer with local administrator credentials.

To set ownership of the TPM

1. Launch the TPM Initialization Wizard. See earlier in this guide.
2. From the Create the TPM owner password dialog box, select **Automatically create the password (recommended)**.
3. From the Save your TPM owner password dialog box, click **Save** and select a location to save the password.

Important We highly recommend saving the TPM ownership password to removable media.

4. Click **Save** again. The password file is saved as *computer_name.tpm*.
5. Click **Print** if you want to print a hard copy of your password.

Important We highly recommend printing a hard copy of your recovery key password and storing it in a safe location.

6. Click **Initialize**.

Note The process of initializing the TPM may take a few minutes to complete.

7. Click **Close**.

Caution Do not lose your password. If you do, you will be unable to make administrative changes until you clear the TPM.

Scenario 2 Turn off and clear TPM

This scenario covers two common tasks that administrators would perform during a re-configuration or recycling of a TPM-equipped computer. These tasks are turning off the TPM and clearing the TPM.

Turn off the TPM

Some administrators may decide that not every TPM-equipped computer in their network needs have the additional protection a TPM provides. In this situation, it is best to ensure that the TPMs in those computers are turned off. The following procedure steps you through the process of turning off the TPM.

Note

A physical presence is not required to turn off the TPM.

To perform the following procedure, you must be logged into a TPM-equipped computer with local administrator credentials.

To turn off the TPM

1. Click **Start**, click **Accessories**, and then click **Run**.
2. Type *tpm.msc* in the **Open** box, and then click **Enter**. The TPM Management Console is displayed.
3. Under **Actions**, click **Turn TPM Off**.
4. From the Turn off the TPM Security Hardware dialog box, select a method for entering your password and turning off the TPM:
 - If you have the removable media onto which you saved your TPM owner password, insert it and click **I have a backup file with the TPM owner password**. From the **Select backup file with the TPM owner password** dialog box, use **Browse** to point to the .tpm file saved on your removable media and click **Open**, and then click **Turn TPM Off**.
 - If you do not have the removable media onto which you saved your password, click **I want to type the TPM owner password**. From the **Type your TPM owner password** dialog box, enter your password (including dashes) and click **Turn TPM Off**.
 - If you do not know your TPM owner password, click **I don't have the TPM owner password**, and follow the instructions provided to turn off the TPM without entering the password.

Note You can turn off the TPM and perform a limited number of management tasks without entering the TPM owner password by just being present at the computer.

The status of your TPM is displayed under **Status** on the TPM Management console.

Clear the TPM

Clearing the TPM cancels the TPM ownership and turns the TPM off. This should be done when a TPM-equipped client computer is recycled, or when the TPM owner has lost their TPM owner password and recovery information was not backed-up. The following procedure steps you through the process of clearing the TPM.

Note

A physical presence is not required to clear the TPM.

To perform the following procedure, you must be logged into a TPM-equipped computer with local administrator credentials.

To clear the TPM

1. Click **Start**, click **Accessories**, and then click **Run**.
2. Type *tpm.msc* in the **Open** box, and then click **Enter**. The TPM Management Console is displayed.

Caution Clearing the TPM resets it to factory defaults and turns it off. You will lose all created keys and data protected by those keys.

3. Under **Actions**, click **Clear TPM**.
4. From the **Clear the TPM Security Hardware** dialog box, select a method for entering your password and clearing the TPM:
 - If you have the removable media onto which you saved your TPM owner password, insert it and click **I have a backup file with the TPM owner password**. From the **Select backup file with the TPM owner password** dialog box, use **Browse** to point to the .tpm file saved on your removable media and click **Open**, and then click **Clear TPM**.
 - If you do not have the removable media onto which you saved your password, click **I want to type the TPM owner password**. From the **Type your TPM owner password** dialog box, enter your password (including dashes) and click **Clear TPM**.

- If you do not know your TPM owner password, click **I don't have the TPM owner password**, and follow the instructions provided to clear the TPM without entering the password.

Note You can clear the TPM and perform a limited number of management tasks without entering the TPM owner password by just being present at the computer.

The status of your TPM is displayed under **Status** on the TPM Management console.

Scenario 3: Block and allow TPM commands

This scenario details the procedure to block or allow a TPM command. This is a task that local administrators may perform during the setup or re-configuration of a TPM-equipped computer. TPM commands are managed through a child node of the TPM Management console named Command Management. Here, administrators can explore the commands available to the TPM. They can also block and allow those commands within the constraints of the Local Machine and Group Policy settings. The following procedure steps you through blocking and unblocking TPM commands.

Note

To perform the following procedure, you must be logged into a TPM-equipped computer with local administrator credentials.

To block and allow TPM commands

1. Click **Start**, click **Accessories**, and then click **Run**.
2. Type *tpm.msc* in the **Open** box, and then click **Enter**. The TPM Management console is displayed.
3. Click **Command Management** in the console tree. A list of TPM commands is displayed.
4. Select a command from the list that you want to block or allow.
5. Under **Actions**, click either **Block Selected Command** or **Allow Selected Command** as needed.

Note Local administrators cannot allow TPM commands blocked through Group Policy.

Logging bugs and feedback

Since TPM Services is a new feature set in Windows Vista, we are very interested in your feedback on your experiences with TPM Services, problems you encountered and the usefulness of the documentation.

When you log bugs, use the instructions on the [Microsoft Connect Web site](http://go.microsoft.com/fwlink/?LinkId=49779) (<http://go.microsoft.com/fwlink/?LinkId=49779>). We are also interested in requests and general feedback about TPM Services.

General feedback and requests for TPM Services can be sent to tpminfo@microsoft.com.

Additional resources

The following resources provide additional information about TPM Services:

- If you need product support, see the [Microsoft Connect Web site](http://go.microsoft.com/fwlink/?LinkId=49779) (<http://go.microsoft.com/fwlink/?LinkId=49779>).
- To access newsgroups for TPM Services, follow the instructions that are provided on the [Microsoft Connect Web site](http://go.microsoft.com/fwlink/?LinkId=50067) (<http://go.microsoft.com/fwlink/?LinkId=50067>).

Technology Adoption Program support

If you are a beta tester and part of the special Technology Adoption Program (TAP) beta program, you can also contact your appointed Microsoft development team member for assistance.