Securing Dell Commercial Client Systems with Trusted Platform Module (TPM) using Dell Client Command Suite

Dell Command | Configure
Dell Command | Monitor
Dell Command | PowerShell Provider

Dell Engineering
July 2017

A Dell Technical White Paper

Revisions

Date	Description
July 2017	Initial release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.
Copyright © 2017 Dell Inc. All rights reserved. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of contents

Executive summary

This white paper describes how system administrators can use Dell Command Suite for configuring the Trusted Platform Module (TPM). It also describes the various BIOS options related to TPM provided in Dell's commercial client systems.

1 Introduction

Trusted Platform Module (TPM) is a chip that provides hardware-based security by integrating cryptographic keys into a system. TPM performs system authentication by using the unique and secret RSA key which is burned into the chip while manufacturing. Moving the security to the hardware layer provides more protection than a software-only solution. Each TPM chip contains the Endorsement Key (EK) which is a RSA key pair. This is maintained inside the chip and cannot be accessed by the software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.

Dell commercial client systems display the TPM settings in BIOS Setup if the TPM is installed on the system and is unhidden. The TPM settings displayed in BIOS Setup depends on the type of TPM that is installed–TPM 1.2 Security or TPM 2.0 Security. TPM 1.2 supports a single "owner" authorization with an RSA 2048b Endorsement Key (EK) for signing or attestation, and a single RSA 2048b Storage Root Key (SRK) for encryption. TPM 2.0 has the same functionality represented by the EK for signing or attestation and SRK for encryption in 1.2, but the control is split into two different hierarchies–the Endorsement Hierarchy (EH) and the Storage Hierarchy (SH).

If the system does not have a physical TPM or the TPM is hidden, the TPM settings option is not displayed in BIOS Setup.

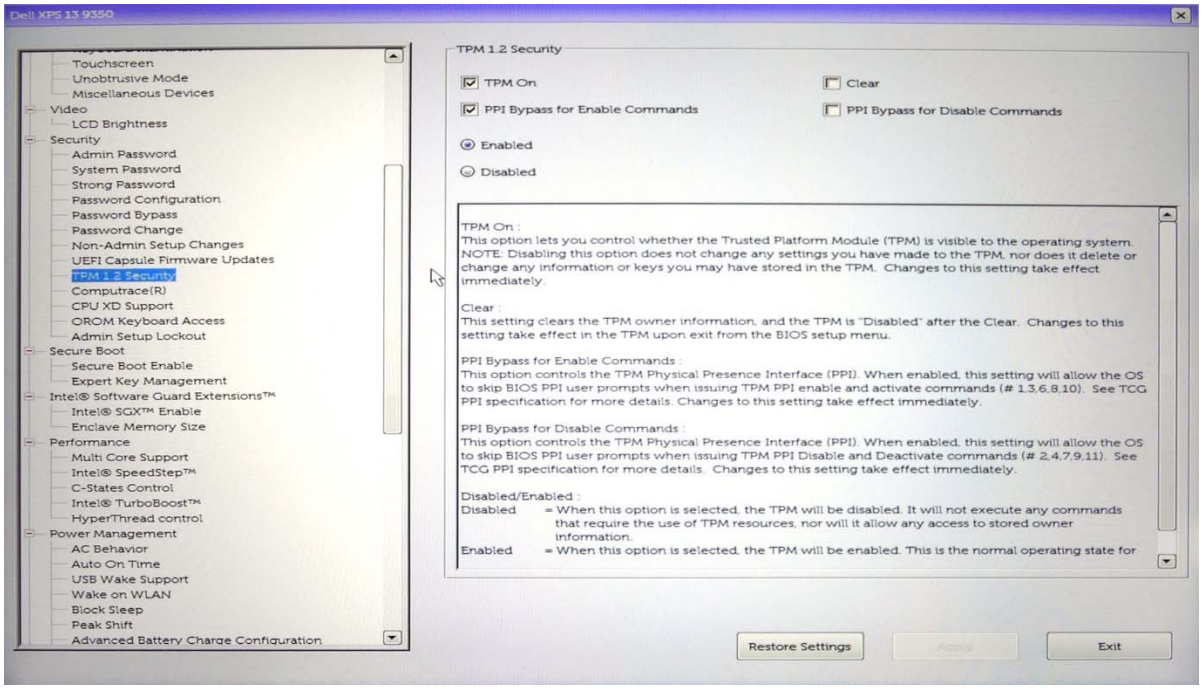

Figure 1 TPM 1.2 settings

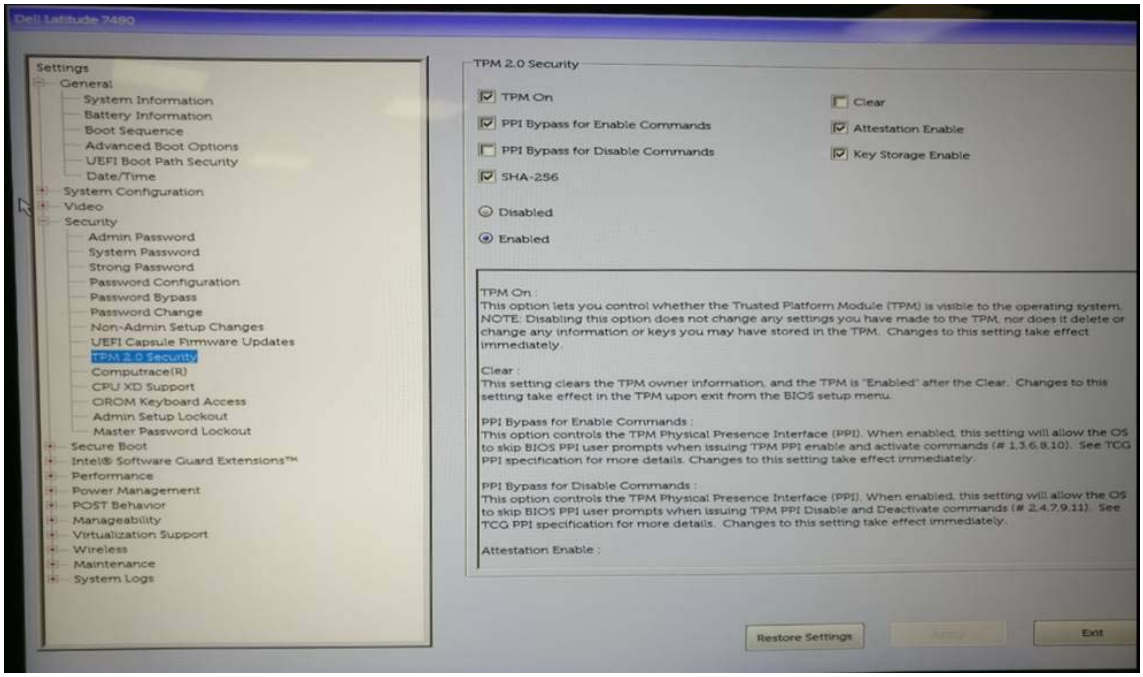

Figure 2 TPM 2.0 settings

The following table describes the various features available in TPM 1.2 and TPM 2.0. Attestation, key storage and SHA-256 options are supported only in TPM 2.0.

Table 1 TPM 1.2 and TPM 2.0 features comparison

Features	Description	TPM 1.2	TPM 2.0
TPM On	Controls the presence of the TPM to the operating system.	Yes	Yes
Enabled/Disabled	Enables and disables the TPM from controlling the execution of commands that utilize the TPM resources.	Yes	Yes
Clear	Clears the TPM ownership information. It returns the TPM to the default state. For TPM 1.2, the TPM is disabled after the clear operation, and for TPM 2.0, the TPM is enabled after the clear operation.	Yes	Yes
PPI Bypass for Enable Commands (TPM PPI Provision Override)	Controls the TPM physical presence interface (PPI). If this option is enabled, physical presence is not required to perform enable and activate operations and the operating system skips the BIOS PPI user prompts while issuing TPM PPI enable and activate commands.	Yes	Yes
PPI Bypass for Disable Commands (TPM PPI De-Provision Override)	Controls the TPM physical presence interface (PPI). If this option is enabled, physical presence is not required to perform disable and deactivate operations	Yes	Yes

	and the operating system skips the BIOS PPI user prompts while issuing TPM PPI disable and deactivate commands.		
Attestation Enable (TPM 2.0 Only)	Controls whether the TPM Endorsement Hierarchy is available to the operating system. Disabling this option restricts the ability to use the TPM for signing and signature operations.	No	Yes
Key Storage Enable (TPM 2.0 Only)	Controls whether the TPM Storage Hierarchy is available to the operating system. Disabling this option restricts the ability to use the TPM for storing owner data.	No	Yes
SHA-256 (TPM 2.0 Only)	Controls the type of hash algorithm that is used by the TPM. If this option is selected, the BIOS and the TPM use the SHA-256 hash algorithm to extend measurements into the TPM PCRs during BIOS boot. If this option is not selected, the BIOS and the TPM use the SHA-1 hash algorithm.	No	Yes

Note: TPM On works as a master switch for other TPM settings. If **TPM On** is not selected, you cannot configure any other settings.

Note: When the TPM **Clear** option is selected, you are prompted for confirmation and a restart is required for completing the operation. After restarting the system, the TPM ownership information (data/keys) is cleared.

Note: Turning TPM Off (clearing the **TPM On** option) does not clear the ownership information.

Note:

You can switch between TPM 1.2 and 2.0. For more information please refer to following links.

http://en.community.dell.com/techcenter/enterprise-client/w/wiki/11850.how-to-change-tpm-modes-1-2-2-0

http://en.community.dell.com/techcenster/enterprise-client/w/wiki/11848.client-tpm

2 Important considerations

- TPM cannot be disabled or deactivated using Dell Command Suite of products. Disabling or deactivation of the TPM can only be performed using the BIOS Setup.
- TPM can be activated or enabled using Dell Command Suite of products only in the following scenarios:
  - Administrator password is set on system.
  - TPM is not owned
  - TPM is disabled or deactivated.
- Dell Command Suite of products do not support configuring the following options. You can configure these options only using the BIOS Setup.
  - TPM Clear
  - Attestation Enable
  - Key Storage Enable

Note: The default setting for TPM 1.2 is “Off” and “Deactivated”.

Note: The default setting for TPM 2.0 is “On” and “Activated”.

Note: You can also use tpm.msc (Windows operating system capability) to clear the TPM.

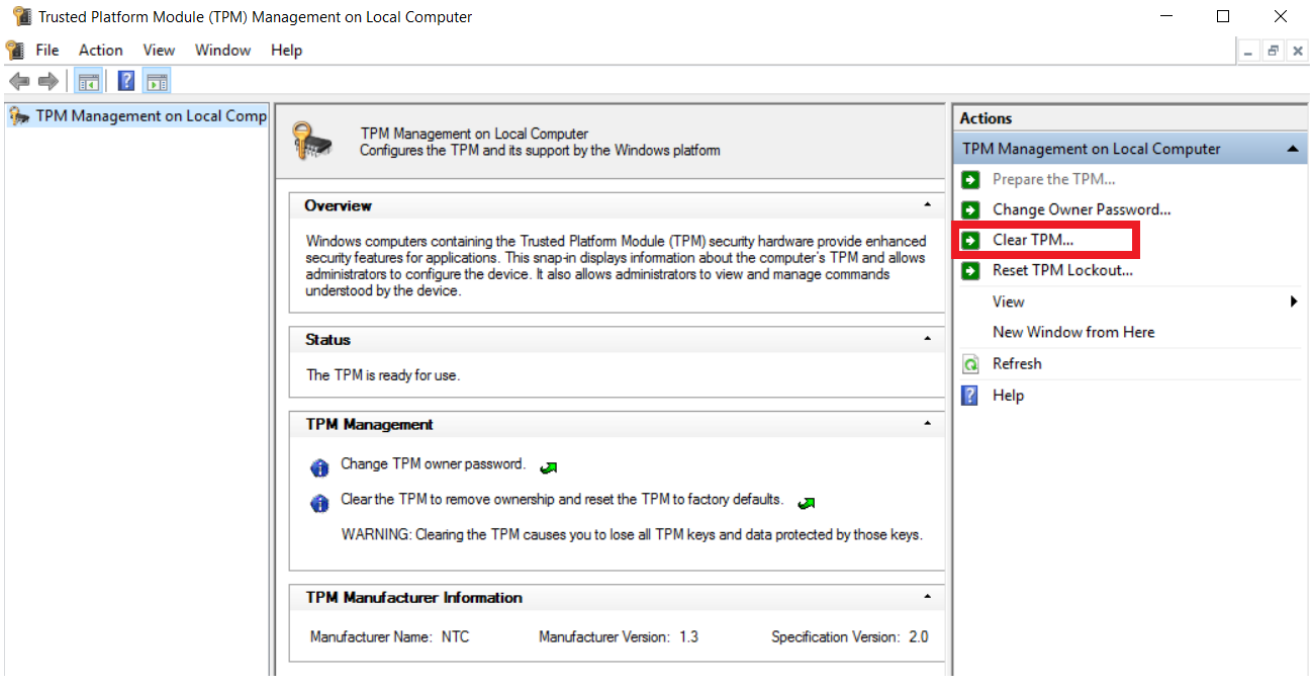

Figure 3 Clearing the TPM using tpm.msc

3 Configuring TPM using Dell Command | Configure

Dell Command | Configure provides the following options to configure the TPM-related features:

- **tpm** – Possible values to configure “TPM On” are **on** and **off**.
- **tpmactivation** – Possible values to configure TPM activation are **activate** and **deactivated**.
- **tpmppipo** – Possible values to configure “PPI Bypass for Enable Commands” are **enable** and **disable**.
- **tpmppidpo** – Possible values to configure “PPI Bypass for Disable Commands” are **enable** and **disable**.
- **tpmhashalgo** – Possible values to configure “SHA-256” are **sha1**, **sha256**, **sha384,** and **sha512**.
- **tpmclear** – Possible values for **tpmclear** are enable and disable.

Note: Deactivated is **read only** value. Deactiavation can be done using BIOS setup.

Note: Tpmclear is read only feature in Dell Command | Configure. TPM Clear can be done using BIOS Setup or Windows utility.

3.1 Activating TPM using Dell Command | Configure CLI

To activate the TPM:

1. Configure the administrator password.

```
C:\Program Files (x86)\Dell\Command Configure\X86_64>cctk.exe --setuppwd=123456

Password is set successfully.
```

Figure 4 Configuring the administrator or setup password

2. Turn on the TPM.

```
C:\Program Files (x86)\Dell\Command Configure\X86_64>cctk.exe --tpm=on --valsetuppwd=123456
tpm=on
```

Figure 5 Turning on the TPM

3. Restart the system.
4. Activate the TPM.

```
C:\Program Files (x86)\Dell\Command Configure\X86_64>cctk.exe --tpmactivation=activate --valsetuppwd=123456
tpmactivation=activate
```

Figure 6 Activating the TPM

5. Restart the system.

If any of the requirements listed in the **Important considerations** section are not met, Dell Command Configure displays an error as show in the following figure.

```
C:\Program Files (x86)\Dell\Command Configure\X86_64>cctk.exe --tpmactivation
tpmactivation=deactivated

C:\Program Files (x86)\Dell\Command Configure\X86_64>cctk.exe --tpmactivation=activate

Error in Setting the Value.
Note: To set TPM - 1. Admin Password must be set , 2. TPM must not be owned and 3. TPM must be deactivated.
```

Figure 7 TPM activation error

You can also see the error code by using echo %ERRORLEVEL% command.

```
C:\Program Files (x86)\Dell\Command Configure\X86_64>echo %ERRORLEVEL%
262
```

Figure 8 Error code

3.2 Activating TPM using Dell Command | Configure GUI

To activate TPM, you must create two separate self-contained executable (SCE) packages.

The first SCE package contains the settings for:

- Configuring the administrator password
- Turning on the TPM

The second SCE package contains the settings for:

- Activating the TPM
- Clearing the password (optional)

3.2.1 Creating SCE package for configuring administrator password and turning TPM on

1. Open the Dell Command | Configure GUI.
2. Select **Create MultiPlatform Package**.
   a. Perform the following steps to turn on the TPM:
      i. Search for **tpm**.
      ii. Click **Edit** or double-click the option.
      iii. From the **Value to Set** list, select the value as “**On**” for tpm.
      The corresponding **Apply Settings** check box is selected automatically.

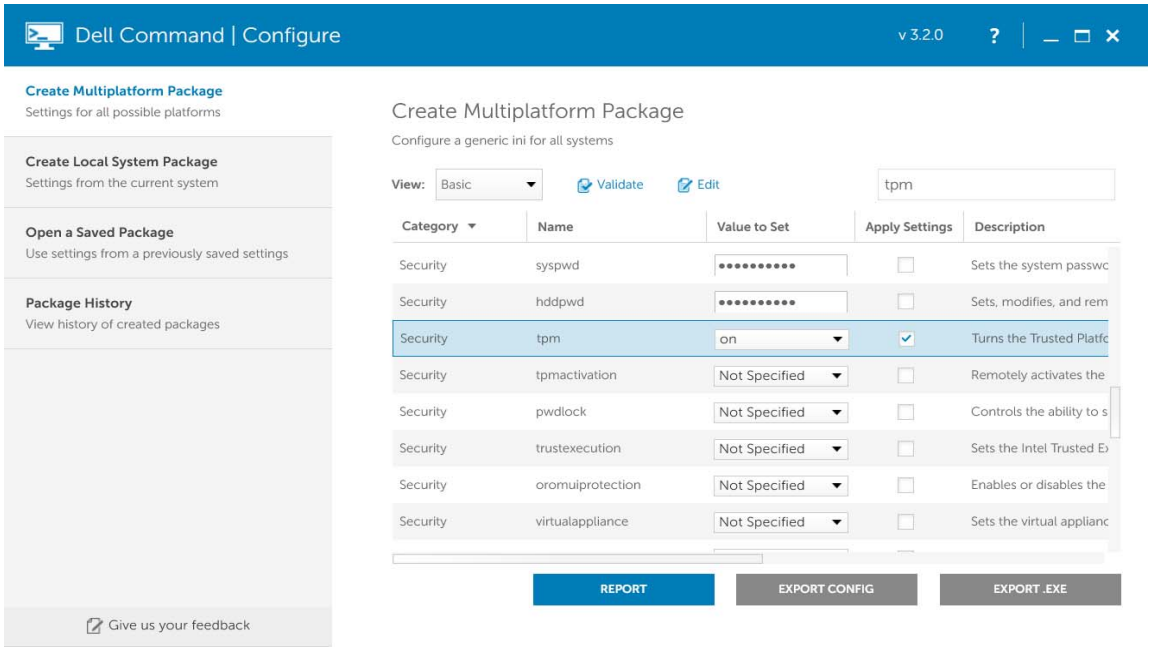

Figure 9 Configuring tpm as on

b. Perform the following steps to configure the administrator or setup password:
   i. Search **setuppwd.**
   ii. In the **Edit** mode, click **Value to Set** field.
   iii. Enter the password.

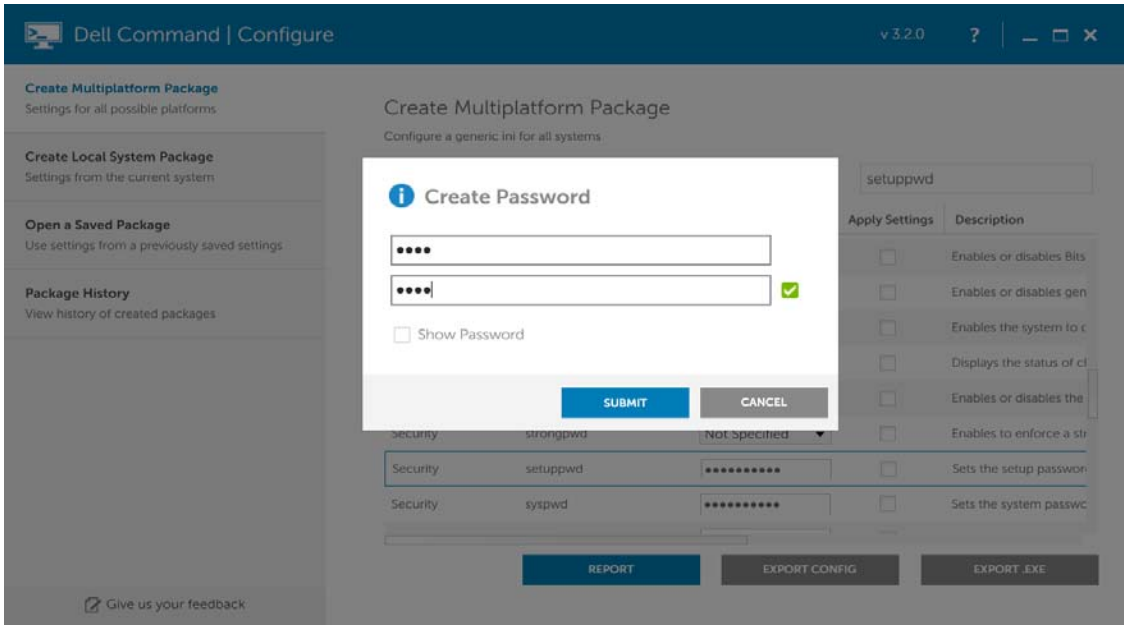

Figure 10 Configuring the administrator password

   iv. Click **Submit**.

3. Click **Export .EXE**.
4. Select **No password is required.**

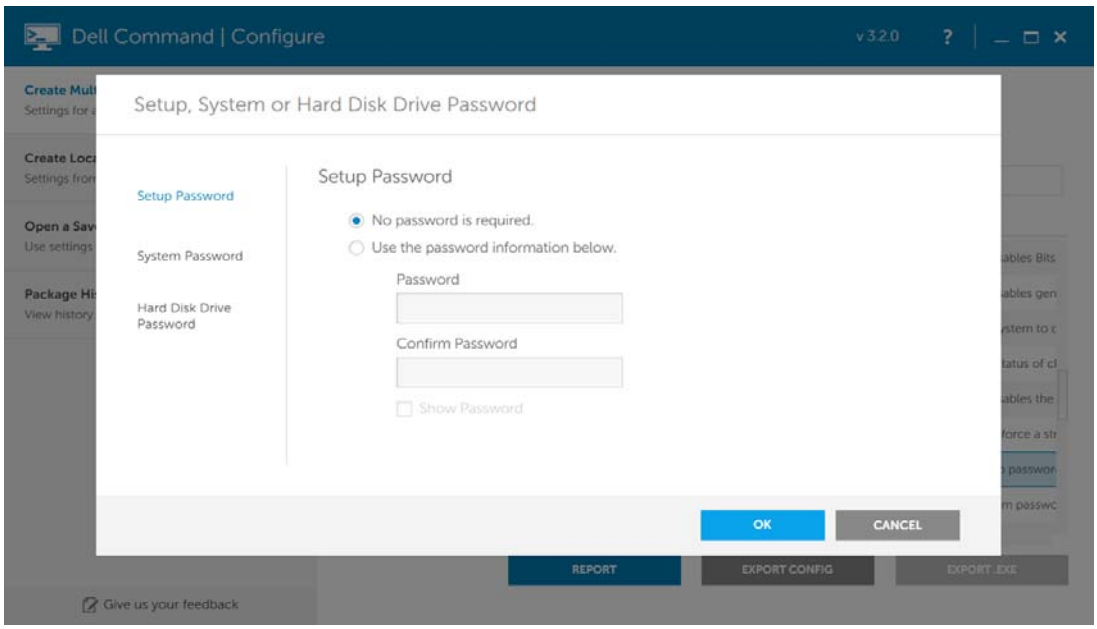

Figure 11 Exporting the SCE package for administrator password and turning tpm on

5. Click **OK** and provide the SCE package file name.

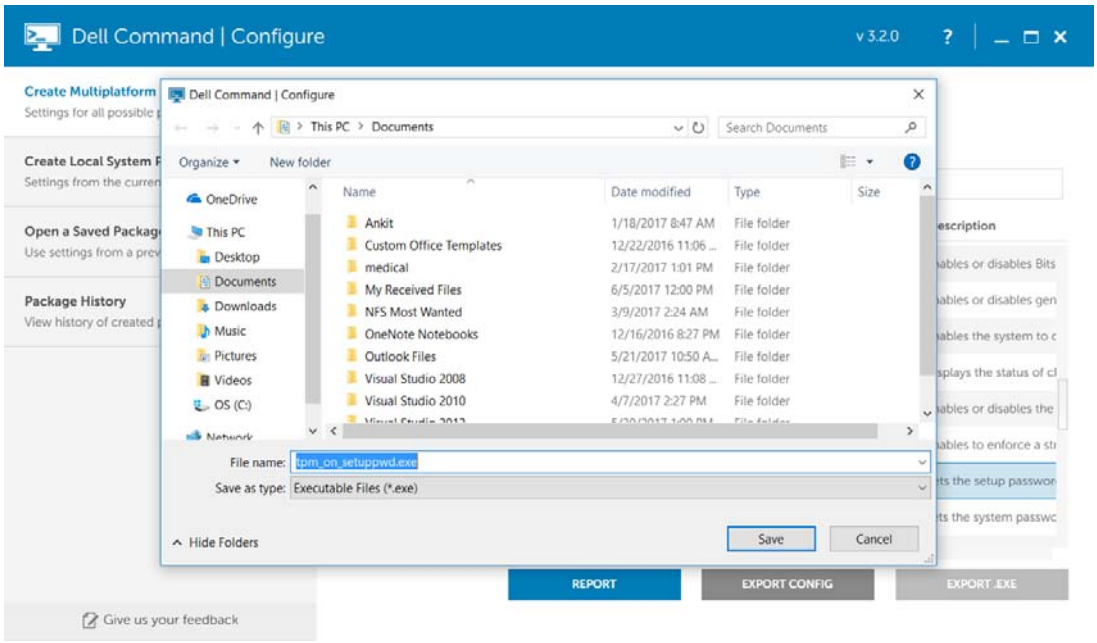

Figure 12 Saving the SCE package file

The first SCE package for configuring the administrator password and turning the TPM on is complete.

3.2.2 Creating SCE package for TPM activation and clearing the setup password

1. Open the Dell Command | Configure GUI.
2. Select **Create MultiPlatform Package**.
   a. Perform the following steps to configure the **tpmactivation.**
      i. Search for **tpmactivation**.
      ii. Click **Edit** or double-click the option.
      iii. From the **Value to Set** drop-down list, select the value as **activate**.
      The corresponding **Apply Settings** check box is selected automatically.

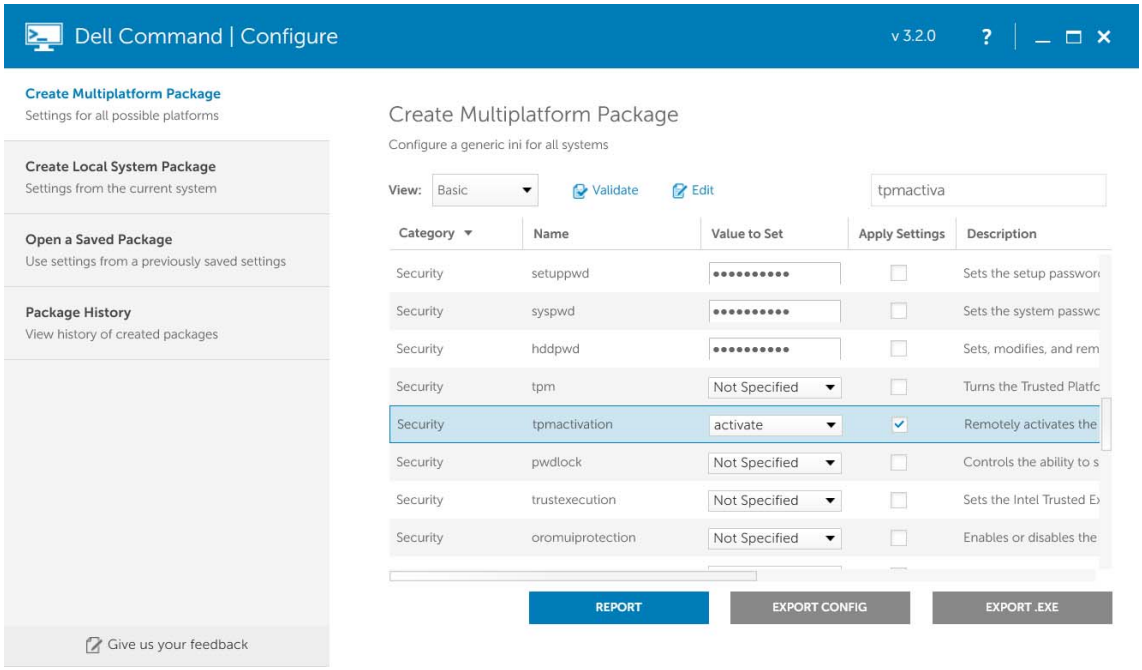

Figure 13 Configuring the tpmactivation

   b. Perform the following steps to clear the setup or administrator password (optional):
      i. Search **setuppwd.**
      ii. In the **Edit** mode, click the **Value to Set** option.
      iii. Enter a blank space in the password text box.
      iv. Enter a blank space in the confirm password text box and then click **Submit**.

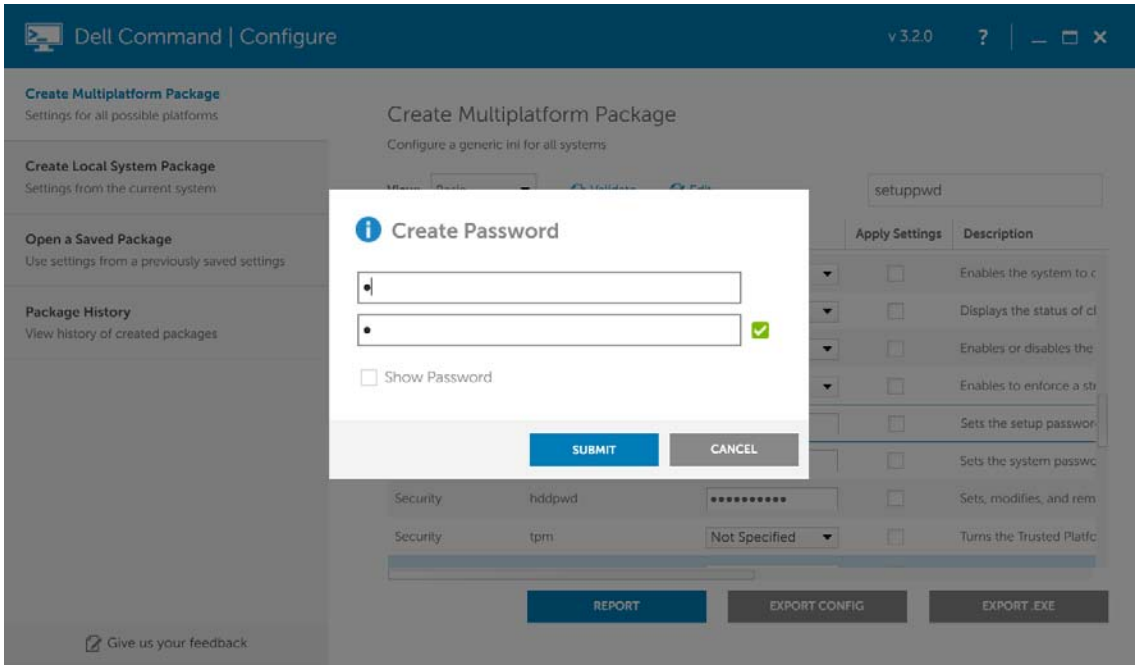

Figure 14 Blank space for clearing the admin password

3. Click **Export .EXE**.
4. Select **Use the password information below** and provide the required password.

Note: Ensure that you provide the same password which you provided during the first SCE package creation.

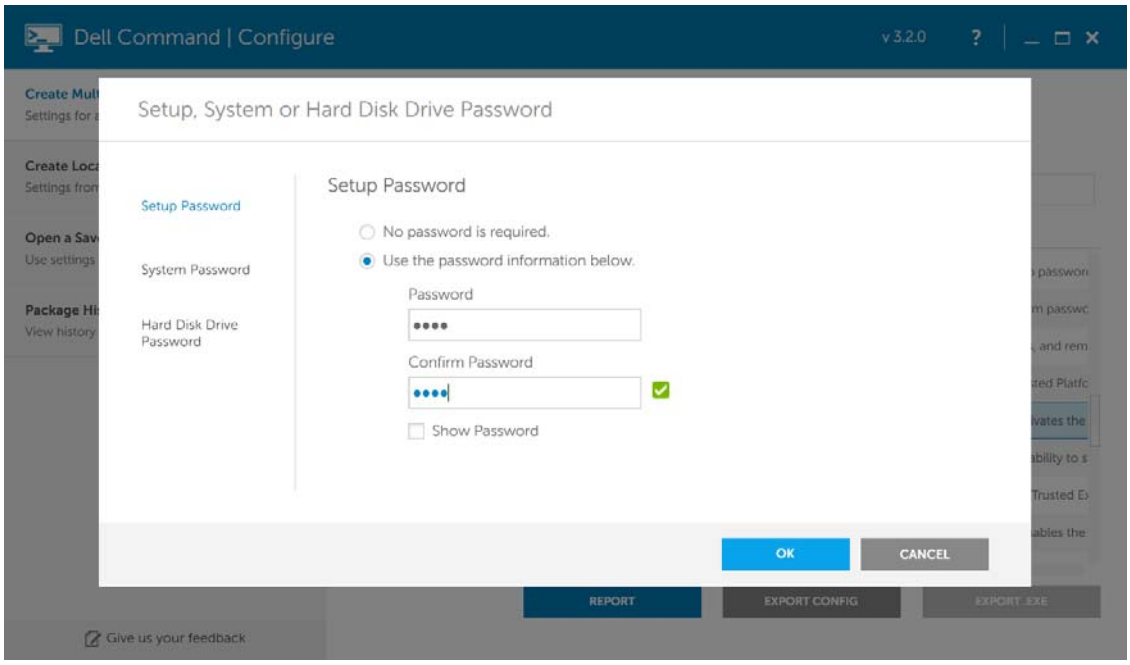

Figure 15 Exporting the SCE package for TPM activation

5. Click **OK** and provide the SCE package file name.

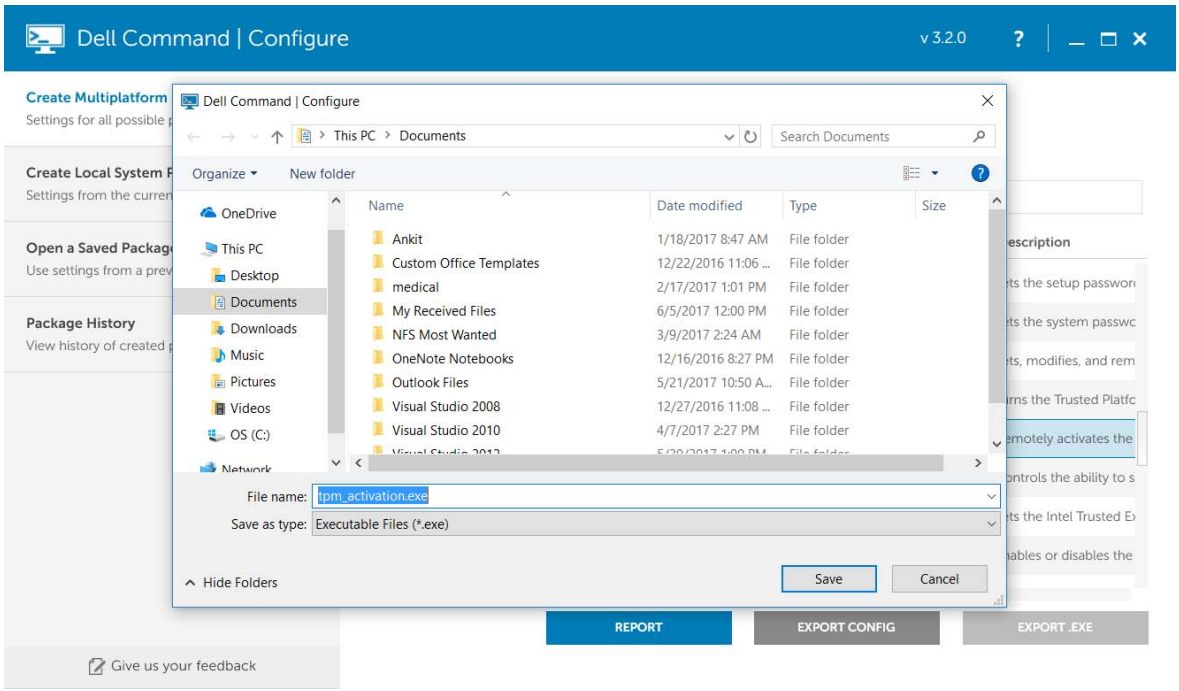

Figure 16 Saving the SCE package file

The second SCE package for tpm activation and clearing the administrator password is complete.

Note: Clearing the administrator password is optional. If you does not want to clear the password, you do not have to perform the steps in section b.

To activate the TPM using SCE package files that were created:

1. Run the first SCE package file that you created for turning TPM on and for configuring the setup or administrator password.
2. Restart the system.
3. Run the second SCE package file that you created for TPM activation and clearing the administrator or setup password.
4. Restart the system.

4 Configuring TPM using Dell Command | PowerShell Provider

Dell Command | PowerShell Provider provides the following options to configure TPM-related features:

- **TpmSecurity** – Possible values to configure “TPM On” are **Enabled** and **Disabled**.
- **TpmActivation** – Possible values to configure TPM activation are **Enabled** and **Disabled**.
- **TpmPpiPo** – Possible values to configure “PPI Bypass for Enable Commands” are **Enabled** and **Disabled**.
- **TpmPpiDpo** – Possible values to configure “PPI Bypass for Disable Commands” are **Enabled** and **Disabled**
- **SHA256** – Possible values for SHA-256 are **Enabled** (to select SHA256), **Disabled** (to select SHA1), **SHA384**, and **SHA512**.
- **TpmClear** – Possible values for TpmClear are **Enabled** or **Disabled**.

Note: TpmActivation cannot be configured to Disabled using Dell Command | PowerShell Provider. It can be disabled using BIOS Setup.

Note: TpmClear is read only feature in Dell Command | PowerShell Provider. TPM Clear can be done using BIOS Setup or Windows utility.

4.1 Activating TPM using Dell Command | PowerShell Provider

To activate the TPM:

1. Configure the administrator password.

```
PS DellSmbios:\Security> si .\AdminPassword "1234" -Verbose
VERBOSE: Performing the operation Set-Item on target "Name: DellBIOS:\Security\AdminPassword Value: 1234".
VERBOSE: SUCCESS.
```

Figure 17 Configuring the administrator or setup password

2. Turn on the TPM.

```
PS DellSmbios:\TPMSecurity> si .\TpmSecurity Enabled -Password "1234" -Verbose
VERBOSE: Performing the operation Set-Item on target "Name: DellBIOS:\TPMSecurity\TpmSecurity Value: Enabled".
VERBOSE: Value being Set Using PLDM Interface
VERBOSE: Password type 'Admin' (Setup) is set.
VERBOSE: SUCCESS.
PS DellSmbios:\TPMSecurity>
```

Figure 18 Turning on the TPM

3. Restart the system.
4. Activate the TPM.

```
PS DellSmbios:\TPMSecurity> si .\TpmActivation Enabled -Password "1234" -Verbose
VERBOSE: Performing the operation Set-Item on target "Name: DellBIOS:\TPMSecurity\TpmActivation Value: Enabled".
VERBOSE: Password type 'Admin' (Setup) is set.
VERBOSE: SUCCESS.
PS DellSmbios:\TPMSecurity>
```

Figure 19 Activating the TPM

5. Restart the system.

If any of the requirements listed in the **Important considerations** section are not met, Dell Command PowerShell Provider displays an error as show in the following figure.

```
PS DellSmbios:\TPMSecurity> gi .\TpmActivation

Attribute     ShortDesc CurrentValue
---------     --------- ------------
TpmActivation TPM State Disabled


PS DellSmbios:\TPMSecurity> si .\TpmActivation Enabled -Verbose
VERBOSE: Performing the operation Set-Item on target "Name: DellBIOS:\TPMSecurity\TpmActivation Value: Enabled".
VERBOSE: The SMI call to BIOS ended in error.
si : FAILURE.
At line:1 char:1
+ si .\TpmActivation Enabled -Verbose
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : WriteError: (DellBIOS:\TPMSecurity\TpmActivation:String) [Set-Item], InvalidOperationException
    + FullyQualifiedErrorId : SMBIOSWriteFailed,Microsoft.PowerShell.Commands.SetItemCommand
PS DellSmbios:\TPMSecurity>
```

Figure 20 TPM activation error

5 Configuring TPM using Dell Command | Monitor

Dell Command | Monitor Provider provides the following options to configure TPM-related features:

- **Trusted Platform Module** – Possible values to configure **TPM On** are **Enable** and **Disable**.
- **Trusted Platform Module Activation** – Possible values to configure TPM activation are **Activate** and **Deactivate**.
- **TPM PPI Provision Override** – Possible values to configure 'PPI Bypass for Enable Commands' are **Enable** and **Disable**.
- **TPM PPI Deprovision Override** – Possible values to configure 'PPI Bypass for Disable Commands' are **Enable** and **Disable**.
- **TPM Hash Algorithm** – Possible values for the TPM Hash Algorithm are **SHA-1**, **SHA-256**, **SHA-384,** and **SHA-512**.
- **Trusted Platform Module Clear** – Possible values for clearing the TPM are **Enabled** or **Disabled**.

Note: Trusted Platform Module Activation cannot be configured to Deactivate using Dell Command | Monitor. It can be deactivated using BIOS Setup.

Note: Trusted Platform Module Clear is read only feature in Dell Command | Monitor. TPM Clear can be done using BIOS Setup or Windows utility.

5.1 Activating TPM using Dell Command | Monitor

To activate the TPM:

1. Configure the administrator password.

```
PS C:\> Get-CimInstance -Namespace root\dcim\sysman  -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{
>> AttributeName=@("AdminPwd");AttributeValue=@("dell")}

ReturnValue SetResult PSComputerName
----------- --------- --------------
          0 {0}
```

Figure 21 Configuring the administrator or setup password

2. Turn on the TPM.

```
PS C:\> Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{
>> AttributeName=@("Trusted Platform Module");AttributeValue=@("1");AuthorizationToken="dell"}

ReturnValue SetResult PSComputerName
----------- --------- --------------
          0 {0}
```

Figure 22 Turning on the TPM

3. Restart the system.
4. Activate the TPM.

```
PS C:\> Get-CimInstance -Namespace root\dcim\sysman  -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{
>> AttributeName=@("Trusted Platform Module Activation");AttributeValue=@("2"); AuthorizationToken="dell"}

ReturnValue SetResult PSComputerName
----------- --------- --------------
          0 {0}
```

Figure 23 Activate the TPM

5. Restart the system.

If any of the requirements listed in the **Important considerations** section are not met, Dell Command Monitor displays an error as show in the following figure.

```
PS C:\> Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration | Where-Object {
>> $_.AttributeName -eq "Trusted Platform Module Activation"}


Caption                 :
Description             :
ElementName             :
AttributeName           : Trusted Platform Module Activation
CurrentValue            : {1}
DefaultValue            :
InstanceID              : Root/MainSystemChassis/BIOSSetupParent/BiosSetupTPMACT
IsOrderedList           :
IsReadOnly              : False
PendingValue            :
PossibleValues          : {1, 2}
PossibleValuesDescription : {Deactivate, Activate}
PSComputerName          :


PS C:\> Get-CimInstance -Namespace root\dcim\sysman  -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{
>> AttributeName=@("Trusted Platform Module Activation");AttributeValue=@("2")}

ReturnValue SetResult PSComputerName
----------- --------- --------------
          0 {1}
```

Figure 24 TPM activation error

6 Additional Resources

You can find related documents, white papers, blogs, and videos for the following products at Dell TechCenter.

Dell Command | Configure:
http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7532.dell-command-configure

Dell Command | PowerShell Provider:
http://en.community.dell.com/techcenter/enterprise-client/w/wiki/6901.dell-commandpowershell-provider

Dell Command | Monitor:
http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor