Tpmvscmgr

Article • 09/06/2024 • 12 contributors •

Applies to: Windows 11, Windows 10, Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016

Feedback

In this article

> ⚠ **Warning**
>
> Windows Hello for Business and FIDO2 security keys are modern, two-factor authentication methods for Windows. Customers using virtual smart cards are encouraged to move to Windows Hello for Business or FIDO2. For new Windows installations, we recommend Windows Hello for Business or FIDO2 security keys.

The Tpmvscmgr command-line tool allows users with Administrative credentials to create and delete TPM virtual smart cards on a computer. For examples of how this command can be used, see Examples.

Syntax

```
Tpmvscmgr create [/quiet] /name <name> /AdminKey {DEFAULT | PROMPT | RANDOM} [/PIN {DEFAULT | PROMPT}] [/PUK {DEFAULT | PROMPT}] [/generate] [/machine <machine name>] [/pinpolicy [policy options]] [/attestation {AIK_AND_CERT | AIK_ONLY}] [/?]

Tpmvscmgr destroy [/quiet] [/instance <device instance ID>] [/machine <machine name>] [/?]
```

Parameters for Create command

The Create command sets up new virtual smart cards on the user's system. It returns the instance ID of the newly created card for later reference if deletion is required. The instance ID is in the format `ROOT\SMARTCARDREADER\000n` where n starts from 0 and is increased by 1 each time you create a new virtual smart card.

Expand table

Parameter	Description
/name	Required. Indicates the name of the new virtual smart card.
/AdminKey	Indicates the desired administrator key that can be used to reset the PIN of the card if the user forgets the PIN. **DEFAULT** Specifies the default value of 010203040506070801020304050607080102030405060708. **PROMPT** Prompts the user to enter a value for the administrator key.

	RANDOM Results in a random setting for the administrator key for a card that is not returned to the user. This creates a card that might not be manageable by using smart card management tools. When generated with RANDOM, the administrator key is set as 48 hexadecimal characters.
/PIN	Indicates desired user PIN value. **DEFAULT** Specifies the default PIN of 12345678. **PROMPT** Prompts the user to enter a PIN at the command line. The PIN must be a minimum of eight characters, and it can contain numerals, characters, and special characters.
/PUK	Indicates the desired PIN Unlock Key (PUK) value. The PUK value must be a minimum of eight characters, and it can contain numerals, characters, and special characters. If the parameter is omitted, the card is created without a PUK. **DEFAULT** Specifies the default PUK of 12345678. **PROMPT** Prompts the user to enter a PUK at the command line.
/generate	Generates the files in storage that are necessary for the virtual smart card to function. If the /generate parameter is omitted, it's equivalent to creating a card without this file system. A card without a file system can be managed only by a smart card management system such as Microsoft Configuration Manager.
/machine	Allows you to specify the name of a remote computer on which the virtual smart card can be created. This can be used in a domain environment only, and it relies on DCOM. For the command to succeed in creating a virtual smart card on a different computer, the user running this command must be a member in the local administrators group on the remote computer.
/pinpolicy	If **/pin prompt** is used, **/pinpolicy** allows you to specify the following PIN policy options: **minlen** <minimum PIN length> If not specified, defaults to 8. The lower bound is 4. **maxlen** <maximum PIN length> If not specified, defaults to 127. The upper bound is 127. **uppercase** Can be **ALLOWED**, **DISALLOWED**, or **REQUIRED.** Default is **ALLOWED.** **lowercase** Can be **ALLOWED**, **DISALLOWED**, or **REQUIRED.** Default is **ALLOWED.** **digits** Can be **ALLOWED**, **DISALLOWED**, or **REQUIRED.** Default is **ALLOWED.** **specialchars** Can be **ALLOWED**, **DISALLOWED**, or **REQUIRED.** Default is **ALLOWED.** When using **/pinpolicy**, PIN characters must be printable ASCII characters.
/attestation	Configures attestation (subject only). This attestation uses an Attestation Identity Key (AIK) certificate as a trust anchor to vouch that the virtual smart card keys and certificates are truly hardware bound. The attestation methods are: **AIK_AND_CERT** Creates an AIK and obtains an AIK certificate from the Microsoft cloud certification authority (CA). This requires the device to have a TPM with an EK certificate. If this option is specified and there's no network connectivity, it's possible that creation of the virtual smart card will fail. **AIK_ONLY** Creates an AIK but doesn't obtain an AIK certificate.
/?	Displays Help for this command.

Parameters for Destroy command

The Destroy command securely deletes a virtual smart card from a computer.

> ⚠ **Warning**
>
> When a virtual smart card is deleted, it cannot be recovered.

Expand table

Parameter	Description
/instance	Specifies the instance ID of the virtual smart card to be removed. The instanceID was generated as output by Tpmvscmgr.exe when the card was created. The **/instance** parameter is a required field for the Destroy command.
/machine	Allows you to specify the name of a remote computer on which the virtual smart card will be deleted. This can be used in a domain environment only, and it relies on DCOM. For the command to succeed in deleting a virtual smart card on a different computer, the user running this command must be a member in the local administrators group on the remote computer.
/?	Displays Help for this command.

Remarks

Membership in the Administrators group (or equivalent) on the target computer is the minimum required to run all the parameters of this command.

For alphanumeric inputs, the full 127 character ASCII set is allowed.

Examples

The following command shows how to create a virtual smart card that can be later managed by a smart card management tool launched from another computer.

Console Copy

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey DEFAULT /PIN PROMPT
```

Alternatively, instead of using a default administrator key, you can create an administrator key at the command line. The following command shows how to create an administrator key.

Console Copy

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey PROMPT /PIN PROMPT
```

The following command will create the unmanaged virtual smart card that can be used to enroll certificates.

Console Copy

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey RANDOM /PIN PROMPT /g
```

The preceding command will create a virtual smart card with a randomized administrator key. The key is automatically discarded after the card is created. This means that if the user forgets the PIN or wants to the change the PIN, the user needs to delete the card and create it again. To delete the card, the user can run the following command.

Console Copy

```
tpmvscmgr.exe destroy /instance <instance ID>
```

where <instance ID> is the value printed on the screen when the user created the card. Specifically, for the first card created, the instance ID is ROOT\SMARTCARDREADER\0000.

The following command will create a TPM virtual smart card with the default value for the administrator key and a specified PIN policy and attestation method:

Console Copy

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /PIN PROMPT /pinpolicy minlen 4
```

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Events

Nov 20, 12 AM - Nov 22, 12 AM

Gain the competitive edge you need with powerful AI and Cloud solutions by attending Microsoft Ignite online.

Register now