

# **Remote Windows Security**

Last Modified on 04.23.24

The **Remote Windows Security** tool lets you view critical security information in your Configuration Manager console. You can also run some actions directly from within Remote Windows Security.

To view security information in your Configuration Manager console, navigate to **Assets and Compliance** > **Devices** > **Right Click Tools** > **Security Tools** > **Remote Windows Security**.

Interested in Remote Windows Security training? Enroll in our Recast Academy course!

## Defender

The **Defender** tab shows information about the status of Windows Defender Antivirus on selected computers.

- Defender Protection (Enabled/Disabled)
- Real-time Protection (Enabled/Disabled)
- Installed antivirus Signature Version
- Installed Defender Client Version
- Installed Defender Engine Version
- Number of Devices in this selection

Expand a section to display the following information for each device selected when running Remote Windows Security.

- Date and time of Last Signature Update
- Date and time of Last Full Scan completion
- Date and time of Last Quick Scan completion

Rem	ote Windows Security - CMDev.	dev.recas	stsoft	ware.com						-		$\times$
Ren	note Windows Securit	t <b>y</b>										
¢ŷ	BitLocker								Refresh	Quick Scar	ı	*
0	ТРМ	$\odot$		Protection	Real-time Protection	Signature Version	Client Version	Engine Version	Devices			
虈	Firmware	٢		Enabled	Disabled	1.331.86.0 Last Signature Upda	4.18.2101.8	1.1.17800.5	1 Quick Scan			
	Virtualization-Based Security				v.recastsoftware.com							
	Defender											
먚;	Defender Exclusions											
	Windows Firewall											
lic	Firewall Rules											
RECA	ST SOFTWARE										0 Erro	rs 🔿

#### **Defender Actions**

- **Quick Scan** (recommended): Scans the locations where malware might be registered to start with the system, such as registry keys and knows Windows startup folders.
- **Full Scan**: Starts with a Quick Scan, then extends the search with a sequential file scan of mounted fixed disks and network drives. A full scan can take hours or days to complete, depending on the amount and type of data included in the scan. If new security intelligence update become available during a full scan, the scan should be repeated to include new threat detections contained in the update.
- **Update Definitions**: Downloads updates to the definition files used to identify malware and other potentially unwanted software.

#### Defender Exclusions

The **Defender Exclusions** tab lists the exclusions applied to selected computers, including the exclusion **Path** and **Type**.

Ren	note Windows Security	y				
<del>C</del> ŵ	BitLocker				Refre	sh
0	ТРМ	⊘     □     Path	Туре	Devices		
Firmware	-	📀 🗌 C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		
	Firmware	🕞 🗌 C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1		
٢	Virtualization-Based Security	🕞 🗌 D:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		
*	Defender	📀 🗌 E\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		
¢		🕞 🗌 F:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		
t,	Defender Exclusions	🕞 🗌 D:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1		_
œ_	Windows Firewall	📀 🗌 E:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1		_
		🕞 🗌 C:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		
<b>UID</b>	Firewall Rules	⊙ □ C:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1		
		D:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		_

## Windows Firewall

The **Windows Firewall** tab display firewall details for selected computers, including whether profiles have been enabled for:

- Domain
- Private
- Public

Expand a section to display more information about an individual firewall profile. The data shown can help determine the inbound and outbound communications allowed on each device and which ports are used. This is also where you can see if logging is enabled and where logs are located.

Remote Windows Security - CM	Dev.dev.recastsoftware.com -	$\Box$ ×
Remote Windows Sec	urity	
BitLocker		Refresh
П трм		
Firmware	⊙     □     □ Domain     Enabled     1	
Virtualization-Based Securi	Image: Weight of the standard stan	
Defender		
Defender Exclusions		
Windows Firewall		
Firewall Rules		
RECAST SOFTWARE		0 Errors 🔿

#### Firewall Rules

This tab displays Windows firewall rules applied to selected computers.

Details include:

- Action: Allow / Block
- Direction: Inbound / Outbound
- Profiles: All, Domain, Private, Public
- Firewall rule Enabled or Disabled
- Number of Devices in this selection

Expand the section for each rule to see the devices on which the rule is applied.

Rem	note Windows Security - CMDev.d	ev.recastsoftware.com	-		×
Rer	note Windows Security	, ,			
¢	BitLocker			Refres	h
0	TPM	⊘ □ Display Name Action Direction Profiles	Enabled	Devices	
1	Firmware	⊙         □         SNMP Trap Service (UDP In)         Allow         Inbound         Private and	d Public Disabled	1	^
		SNMP Trap Service (UDP In) Allow Inbound Domain	Disabled	1	
\$	Virtualization-Based Security	O         □         WFD Driver-only (TCP-In)         Allow         Inbound         All	Enabled	1	
*	Defender	⊘ □ WFD Driver-only (TCP-Out) Allow Outbound All	Enabled	1	
		Second Se	Enabled	1	
넃	Defender Exclusions	WFD Driver-only (UDP-Out)     Allow Outbound All	Enabled	1	_
	Windows Firewall	Delivery Optimization (TCP-In)     Allow Inbound All	Enabled	1	
		🕞 🗌 Delivery Optimization (UDP-In) Allow Inbound All	Enabled	1	
J	Firewall Rules	🕑 🗌 Windows Collaboration Computer Name Registration Service (PNRP-In) Allow Inbound All	Disabled	1	_
		(♥) □ Windows Collaboration Computer Name Registration Service (PNRP-Out) Allow Outbound All	Disabled	1	~
RECA	IST SOFTWARE			0 Error	5 ( )

### BitLocker

View the current protection status for the drives on selected computers.

Details include:

- Associated Drive Letter
- Protection Status for the drive
- Encryption Method for the drive
- Conversion Status for the drive, if encrypted
- Key Protectors used for this drive
- Volume Type for this drive
- Number of devices in this selection

Expand the section for each drive to see details about the Disk Size in GB, Encryption Percentage, and Lock status.

🏮 Ren	note Windows Security - CMDev.	dev.recas	stsoftware.com							_		×
Rei	mote Windows Securit	t <b>y</b>										
С Э	BitLocker					Refresh		Suspend Y	Backup F	Recovery Passw	ord to AD	*
0	трм	$\odot$	Drive Letter	Protection Status	Encryption Met	nod Conve	sion Status	Key Protectors		Volume Type	Devices	
躑	Firmware	$\odot$	C:	Protected	XTS-AES 256 Disk Size (GB)		crypted	TPM, NumericRecove	eryPassword	System	1	
<b>\$</b>	Virtualization-Based Security			recastsoftware.com		100	rercentage	Unlocked				
۲	Defender											
<b>먇</b> ;	Defender Exclusions											
<b>₽</b>	Windows Firewall											
<b>U</b>	Firewall Rules											
RECA	IST SOFTWARE										0 Erro	ors 🔿

**BitLocker Actions** 

• Suspend or Resume BitLocker encryption

- **Decrypt** or **Encrypt** the content of the volume.
  - A confirmation prompt appears before decryption begins.
  - When you click **Encrypt**, the Right Click Tools Encryption Wizard will open and you'll be asked to choose options such as encryption method and its scope.
- Backup Recovery Password to AD: Saves the password to Active Directory Domain Services.
- Backup Recovery Password to Azure : Saves the password to Azure Active Directory (Entra ID) Domain Services.
- Force Recovery on Next Restart: Forces the user to enter the recovery key upon device restart.
- Regenerate Recovery Password: Generates a new recovery password.

#### TPM

The **TPM** tab shows information about the status of the Trusted Platform Module on selected computers.

Included details:

- Trusted Computing Group (TCG) Version
- TPM Activated (T/F)
- TPM Enabled (T/F)
- TPM Owned by the OS (T/F)
- TPM Ready (T/F)
- Number of Devices in this selection

Expand a section to display Manufacturer and Manufacturer Version details, as well as whether the device is FIPS Ready or Locked Out.

Rem	note Windows Security - CMDev.o	dev.reca	stsoft	tware.com									-		$\times$
Rer	note Windows Securit	y													
ŝ	BitLocker										Refresh	(	Clear TPM		*
6	ТРМ	$\odot$		TCG Version	Activated	Enabled	Owned	Ready	Devices						
躑	Firmware	$\odot$		2.0, 0, 1.16	True	True	True	True	1	5100.0					
	Virtualization-Based Security			Name CMDev.dev.	recastsoftw				Nanufacturer Version 213.275.21.18466	False	False				
۲	Defender														
<b>F</b> .	Defender Exclusions														
	Windows Firewall														
<b>II</b> C	Firewall Rules														
~															
RECA	ST SOFTWARE													0 Erro	rs 🔿

#### **TPM Actions**

**Clear TPM**: Resets the TPM to its default state. This function removes the owner authorization value and any keys stored in the TPM.

Provision TPM: Executes part of the provisioning process which prepares a TPM for use.

Enable Auto-Provisioning: Allows TPM provisioning to happen during auto-provisioning.

### Firmware

The Firmware tab shows information about specific security settings related to selected computers.

Included details:

- Unified Extensible Firmware Interface (UEFI) Enabled (T/F)
- SecureBoot Enabled (T/F)
- Number of Devices in this selection

Remote Windows Security - CMDev.	ev.recastsoftware.com	- 🗆	×
Remote Windows Securit			
BitLocker	Refresh		*
Ф трм	O UEFI Enabled SecureBoot Enabled Devices		
Firmware	True True 1		
Virtualization-Based Security	CMDev.dev.recastsoftware.com		
Defender			
Defender Exclusions			
Windows Firewall			
Firewall Rules			
RECAST SOFTWARE		0 En	rors 🔿

#### Virtualization-Based Security

This tab shows information about virtualization-based security options for selected computers.

Included details:

- Virtualization-Based Security (VBS) Enabled (T/F)
- VBS Platform Security Features
- Credential Guard Enabled
- System Guard Enabled (T/F)
- Number of Devices in this selection

Ren	note Windows Security - CMDev.	dev.recast	tsoftware.com				-		×
Rer	note Windows Securit	у							
<del>C</del>	BitLocker				Refresh Ena	ble Credential Guard	✓ DMA Protection	UEFI	Lock
0	TPM	$\odot$	VBS Enabled	VBS Platform Security Features	Credential Guard Enabled	System Guard Enabled	Devices		
鞹	Firmware	$\odot$	True Name	Secure Boot and DMA Protection	Enabled with UEFI lock	True	1		
<b>:</b>	Virtualization-Based Security		CMDev.dev.n	ecastsoftware.com					
۲	Defender								
먲	Defender Exclusions								
	Windows Firewall								
<b>II</b> C	Firewall Rules								
~									
RECA	IST SOFTWARE							0 Erro	rs 🔿

Virtualization-Based Security Actions

- Enable Credential Guard
- Enable System Guard
- Enable or disable **DMA Protection**: Enabled by default
- Enable or disable **UEFI Lock**: Enabled by default

Copyright © 2024 Recast Software Inc. All rights reserved.